Exploitation of RF-DNA for Device Classification and Verification Using GRLVQI Processing

DISSERTATION

Donald R. Reising, DR-II, USAF

AFIT-ENG-DS-12-04

DEPARTMENT OF THE AIR FORCE
AIR UNIVERSITY

AIR FORCE INSTITUTE OF TECHNOLOGY

Wright-Patterson Air Force Base, Ohio

APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED

The views expressed in this dissertation are those of the author and do not reflect the official policy or position of the United States Air Force, the Department of Defense, or the United States Government.

This material is declared a work of the U.S. Government and is not subject to copyright protection in the United States.

AFIT-ENG-DS-12-04

Exploitation of RF-DNA for Device Classification and Verification Using GRLVQI Processing

DISSERTATION

Presented to the Faculty

Graduate School of Engineering and Management

Air Force Institute of Technology

Air University

Air Education and Training Command

In Partial Fulfillment of the Requirements for the

Degree of Doctor of Philosophy

Donald R. Reising, B.S.E.E., M.S.E.E.

DR-II, USAF

December 2012

APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED

AFIT-ENG-DS-12-04

Exploitation of RF-DNA for Device Classification and Verification Using GRLVQI Processing

Donald R. Reising, B.S.E.E., M.S.E.E.
DR-II, USAF

Approved:

Dr. Michael A. Temple (Chairman)	30 Nov 2012 Date
Dr. Julie A. Jackson (Member)	30 Nov 2012 Date
Dr. Mark E. Oxley (Member)	30 Nov 2012 Date

Accepted:

M. U. THOMAS Dean, Graduate School of Engineering and Management	18 Dec 2012 Date

Abstract

To provide reliable, accurate, and timely wireless network security, this work introduces a Generalized Relevance Learning Vector Quantized Improved (GRLVQI) classification process and extends applicability of RF "Distinct Native Attribute" (RF-DNA) fingerprinting for device *classification* (a one-to-many looks "most like" assessment) and device identity *verification* (a one-to-one looks "how much like" assessment). Transition to the GRLVQI process was motivated by earlier RF-DNA fingerprinting work that used a Multiple Discriminant Analysis/Maximum Likelihood (MDA/ML) classification process. Although successful, the earlier MDA/ML works are inherently limited in that they provide no capability for determining which RF-DNA features are most important to classification or identification–GRLVQI inherently provides a feature relevance indication and overcomes this limitation.

GRLVQI feature relevance ranking is exploited here to enable Dimensional Reduction Analysis (DRA) and enhance the experimental-to-operational transition potential of RF-DNA fingerprinting, i.e., identify the minimum number of required RF-DNA features to achieve desired classification and verification performance. This is done using RF-DNA features extracted from 2D (time-frequency) Gabor Transform (GT) responses of experimentally collected emissions from Orthogonal Frequency Division Multiplexing (OFDM) based 802.16 Worldwide Interoperability for Microwave Access (WiMAX) and 802.11 WiFi devices. Performance using 2D GT-based RF-DNA features proves superior relative to demonstrations using 1D Time Domain (TD), 1D Spectral Domain (SD) and 2D Dual-Tree Complex Wavelet Transform (DT-$\mathbb{C}$WT) features.

Using GT-based RF-DNA fingerprints and the GRLVQI classifier, demonstrations here include average classification accuracy of $\%C \geq 90\%$ using 1) 204 full dimensional features from WiMAX emissions at $SNR \geq 10.0$ dB, and 2) 363 full dimen-

sional features from WiFi emissions at $SNR \geq 12.0$ dB. Performance with DRA$\approx$90% dimensionally-reduced feature sets (top ranked 10% of the most relevant features retained) included $\%C \geq 90\%$ using only 1) 20 of 204 WiMAX features at $SNR \geq 12.0$ dB and 2) 36 of 363 WiFi features at $SNR \geq 13.0$ dB. Collectively, this corresponds to a 1.0 to 2.0 dB trade-off in required SNR to achieve a given $\%C$ with an appreciable reduction in required computational resources. For device ID verification using the same DRA$\approx$ 90% GT-based RF-DNA fingerprints, GRLVQI effectively enabled: 1) 100% ID verification of all six *authorized* WiMAX devices while detecting 97% (35 of 36 attempts) of spoofing attacks by unauthorized *rogue* WiMAX devices at SNR=18.0 dB, and 2) 100% ID verification of all four *authorized* WiFi devices at SNR=15.0 dB; rogue WiFi device detection was not assessed due to available data limitations and remains an area of interest for future research.

Acknowledgements

I owe a large debt of gratitude to my research advisor, Dr. Michael Temple, for his patience, guidance, and support throughout this research effort. The technical expertise and advice were insightful, motivational, and immensely appreciated. Throughout this entire effort you have served as a trusted advisor not only technically but also personally and for that I am truly grateful.

I would also like to thank my wife, because without her love, constant encouragement, understanding, and support none of this would have been possible.

Donald R. Reising

Table of Contents

Page

List of Figures

List of Tables

List of Symbols

Symbol		Page
C_i	Claimed Device ID	42
D_i	Actual Device ID	42
N_z	Number of Monte Carlo Noise Realizations	50
%C	Correct Classification Percentage	50
G_p	Classification Performance Gain in Decibels	50
N_C^R	Number of *Rogue* Network Devices	70
N_z	Number of Monte Carlo Noise Realizations	74
$\mathbf{s}_{LOS}$	Multipath *Line-of-Sight* Signal	88
$\mathbf{s}_{REF}$	Multipath *Reflected* Signal	88
$\mathbf{s}_{MP}$	Received Multipath Signal	88
A_R	Amplitude of Reflected Signal	88
k_R	Reflecte4d Signal Time Delay	88
M#	Multipath *Model* Development Number	91
T#	RF-DNA Fingerprint *Testing* Set Number	91

List of Abbreviations

Abbreviation		Page
OFDM	Orthogonal Frequency Division Multiplexing	1
IEEE	Institute of Electrical and Electronics Engineers	1
WiFi	Wireless Fidelity	1
WiMAX	Worldwide Interoperability for Microwave Access	1
3GPP	3rd Generation Partnership Project	1
LTE	Long Term Evolution	1
WAP	Wireless Access Points	2
IT	Information Technology	2
ICS	Industrial Control System	2
SCADA	Supervisory Control And Data Acquisition	2
EMS	Energy Management System	2
FAA	Federal Aviation Administration	2
ICAO	International Civilian Aviation Organization	2
OSI	Open Systems Interconnection	2
NWK	Network	2
DLL	Data Link	2
PHY	Physical	3
RF	Radio Frequency	3
ID	Identity	3
GSM	Global System for Mobile Communications	4
RFID	Radio Frequency Identification	4
RF-DNA	Radio Frequency-Distinct Native Attributes	4
DT-ℂWT	Dual-Tree ℂomplex Wavelet Transform	5
TD	Time Domain	5
SD	Spectral Domain	5
T-F	Time-Frequency	5

Abbreviation		Page
GT	Gabor Transform	5
GWT	Gabor-Wigner Transform	5
FrFT	Fractional Fourier Transform	5
FLD	Fisher's Linear Discriminant	6
kNN	K-Nearest Neighbor	6
SVM	Support Vector Machine	6
MDA	Multiple Discriminant Analysis	6
ML	Maximum Likelihood	6
AFIT	Air Force Institute of Technology	7
ANN	Artificial Neural Network	7
GRLVQI	Generalized Relevance Learning Vector Quantization-Improved	7
LFS	Learning From Signals	7
ORNL	Oak Ridge National Laboratory	7
MAC	Medium Access Control	9
ESN	Electronic Serial Number	9
IMEI	International Mobile Equipment Identity	9
SIM	Subscriber Identity Module	9
ROC	Receiver Operating Characteristic	9
EER	Equal Error Rate	9
FRR	False Reject Rate	9
FAR	False Accept Rate	9
TDD	Time Division Duplexing	12
BTS	Base Transciever Station	12
DL	Down-Link	12
MS	Mobile Subscriber	12
UL	Up-Link	12
PSD	Power Spectral Density	17
DFT	Discrete Fourier Transform	17

Abbreviation		Page
DGT	Discrete Gabor Transform	19
WVD	Wigner-Ville Distribution	19
DPWD	Discrete Pseudo Wigner Distribution	19
LDA	Linear Discriminant Analysis	21
DRA	Dimensional Reduction Analysis	24
FVR	False Verification Rate	28
TVR	True Verification Rate	28
TRR	True Reject Rate	28
RFSICS	RF Signal Intercept and Collection System	29
AWGN	Additive White Gaussian Noise	29
MDA/ML	Multiple Discriminant Analysis/Maximum Likelihood	29
ID	Identification	29
IF	Intermediate Frequency	29
ADC	Analog-to-Digital Converter	29
Msps	mega-samples-per-second	29
I	In-Phase	29
Q	Quadrature	29
VT	Variance Trajectory	30
VT	Variance Trajectory	31
LOS	Line-of-Sight	88
PMF	Probability Mass Function	89
AFRL/RY	Air Force Research Laboratory Sensors Directorate	103

Exploitation of RF-DNA for Device Classification and Verification Using GRLVQI Processing

I. Introduction

This chapter introduces the dissertation research and its documentation. The operational and technical motivation for conducting the research is provided in Section 1.1 and Section 1.2, respectively. Section 1.2 contains three subsections, including a summary of related work in RF fingerprinting in Section 1.2.1, device *classification* in Section 1.2.2, and device ID *verification* in Section 1.2.3. A relational mapping between prior related research and research contributions of this dissertation is provided in Section 1.3, followed by a document organization overview in Section 1.4.

1.1 Operational Motivation

Historically, opportunistic "hackers" have routinely gained unauthorized access to wireless networks and their malicious activities are expected to continue as new technologies emerge [10,11,15]. Given the ubiquity of Orthogonal Frequency Division Multiplexing (OFDM) and Institute of Electrical and Electronics Engineers (IEEE) standards governing the following operations,

1. IEEE 802.11a/g Wireless Fidelity (WiFi) operation [51],
2. IEEE 802.16 Worldwide Interoperability for Microwave Access (WiMAX) operation [50, 52], and
3. 3rd Generation Partnership Project (3GPP) Long Term Evolution (LTE) operation [4, 5],

the threat of unauthorized network access remains a concern for OFDM-based wireless networks. This is especially true when considering that WiFi, WiMAX and LTE

networks commonly provide user access through Wireless Access Points (WAP)–one of the top 10 Information Technology (IT) security threats [2].

The concern is even greater when considering applications in which these networks form critical links in an overall system architecture. Some architectures in which OFDM-based wireless networks are deployed, or being considered for deployment, include:

1. Home area WiFi and neighborhood area WiMAX networks in support of Smart Grid maintenance and operation [61, 91].
2. Cloud computing connectivity to facilitate user access to data anywhere at anytime [28]. In cloud-connected wireless networks the end users surrender protective custody of their data; therefore, it is imperative that only *authorized* users be granted access. This is even more critical when considering the potential number of peripherally connected subnetworks operating at or near the "edge" of a larger cloud infrastructure.
3. Industrial Control System (ICS), Supervisory Control And Data Acquisition (SCADA), Energy Management System (EMS), and other critical infrastructure elements. The backbone and/or backhaul communication for these type of systems is commonly based on the IEEE WiMAX standards and their security is paramount to national security [61, 80].
4. Other public safety applications such as the WiMAX-based AeroMAX network being developed by the Federal Aviation Administration (FAA), Eurocontrol, and International Civilian Aviation Organization (ICAO) to support next generation airport communication services [32, 37].

Services provided within wireless networks are characterized and standardized by the Open Systems Interconnection (OSI) model that is comprised of seven layers as shown in Fig. 1.1. Security and detection of unauthorized users has been traditionally addressed within higher "bit-level" layers of the OSI model, e.g., Network (NWK) and Data Link (DLL) layers. This includes a considerable amount of research conducted

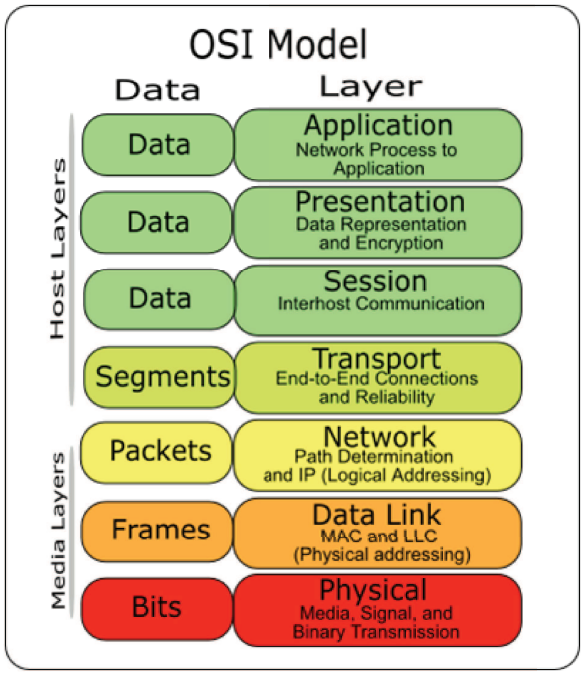


Figure 1.1: Multi-layer Open Systems Interconnect (OSI) network model [1, 3].

on bit-level security mechanisms to detect and/or mitigate unauthorized network access [17, 60, 65, 78, 85, 96]. By design, these higher layer bit-level security approaches inherently ignore the Physical (PHY) layer –the WAP "doorway" through which a majority of malicious activity occurs. Neglecting the PHY layer fails to leverage potentially useful information contained within wireless network Radio Frequency (RF) emissions.

RF fingerprinting is one method that leverages potentially discriminating PHY layer information by exploiting unique features that are 1) unintentionally imparted on RF emissions by hardware components comprising the wireless device, and 2) difficult for unauthorized users to mimic and replicate. RF fingerprints facilitate discrimination between multiple devices, establishment of a device's identity (ID), and mitigation of unauthorized network access. This research investigates the exploitation of PHY layer attributes (i.e., RF fingerprints) as a means for augmenting bit-level security mechanisms to 1) improve authorized user *verification*, and 2) increase detection of unauthorized devices attempting to gain network access. Previous research

has shown that PHY layer attributes can be useful in the identification of wireless devices and provide a means of augmenting current bit-level network security mechanisms. Section 1.2 provides a summary of previously investigated RF fingerprinting techniques that utilize PHY layer attributes to accomplish this goal.

1.2 Technical Motivation

A considerable amount of research has been conducted in the area of RF fingerprinting over the past two decades [23–25, 27, 31, 33, 36, 38–41, 44, 45, 47, 49, 54, 56–58, 67, 71–76, 81, 84, 86, 88, 89, 93–95]. These works have predominalty investigated the use of RF fingerprints for device *classification* (a one-to-many looks "most like" assessment) using various wireless communication devices, including: IEEE 802.11 WiFi [44, 45, 47, 54, 56, 57, 67, 73, 81, 84], Global System for Mobile Communications (GSM) cellular phones [75, 93], IEEE 802.16 WiMAX [71–73, 76, 94], IEEE 802.15 Bluetooth [40], and Radio Frequency Identification (RFID) [23, 95]. The work in [44, 45, 47, 56–58, 71–73, 76, 81, 93, 94] focused on inherent PHY layer benefits that leverage RF 'Distinct Native Attributes' (RF-DNA) extracted from specific portions of modulated signal responses to achieve serial number discrimination. In this context, RF-DNA attributes are 1) sufficiently "distinct" to facilitate persistent cross-device discrimination and 2) "native" in that variations due to hardware implementation, component type, manufacturing processes and/or environmental interactions impart unintentional "coloration" upon the modulated waveform that enable device discrimination.

1.2.1 RF Fingerprinting. While a considerable body of knowledge has been established within the area of RF-DNA fingerprinting, there remained a need at the onset of this research to improve the experimental-to-operational transition potential of RF-DNA fingerprinting and facilitate successful fielding of a system to provide reliable and robust PHY layer security augmentation. The envisioned network addition, designated here as an RF "Air Monitor", must be able to discriminate between 1) de-

vices from different manufacturers (inter-manufacturer discrimination), 2) dissimilar model devices from the same manufacturer (intra-manufacturer discrimination), and 3) like model devices from the same manufacturer (intra-manufacturer serial number discrimination). As repeatedly demonstrated, intra-manufacturer serial number discrimination presents the greatest challenge [44, 47, 57, 76, 93, 94] and three approaches that can be used to improve overall *classification* performance, include:

1. Discovering a *more robust feature set* for use with a given classifier, where increased robustness enables use of a single, minimal dimension feature set under multiple channel conditions (Gaussian, Rayleigh, etc.) and/or multiple device combinations (inter-manufacturer and intra-manufacturer conditions).
2. Developing a *more powerful classifier* for a given feature set, where increased power is indicated by either 1) requiring a lower SNR to achieve a given *classification* level, or 2) achieving a higher *classification* level for a given SNR.
3. A combination thereof.

To improve RF-DNA fingerprinting *classification* performance, related work in [56–58] investigated the use of an alternate feature set generated from 2D Dual-Tree $\mathbb{C}$omplex Wavelet Transform (DT-$\mathbb{C}$WT) coefficients; the first successful transition from 1D Time Domain (TD) and 1D Spectral Domain (SD) feature sets to a 2D joint Time-Frequency (T-F) feature set. The DT-$\mathbb{C}$WT exploits momentary and/or time localized signal energy changes as a function of frequency [55]. Using preamble responses from 802.11a wireless signals, results in [56–58] show that *classification* performance using 2D DT-$\mathbb{C}$WT T-F features is superior when compared with results using 1D TD or SD features. However, the T-F resolution trade-off present in the DT-$\mathbb{C}$WT (i.e., increasing time resolution decreases frequency resolution and visa-versa) was deemed as being potentially limiting.

Among the list of alternative 2D feature spaces initially considered are the linear Gabor Transform (GT), non-linear Gabor-Wigner Transform (GWT) [18, 83], the Fractional Fourier Transform (FrFT) [14, 16, 66, 69], the $\mathbb{S}$-Transform [79], the

Chirplet [63], and the Cohen class of T-F distributions (e.g., Choi-Williams Transform) [21]. GT and GWT feature sets ultimately became the focus for detailed proof-of-concept demonstration given:

1. They both mitigate potentially adverse T-F resolution trade-off effects,
2. They both have been successfully used for assessing power line quality and detecting anomalous signal behavior [18, 83],
3. Technical community "encouragement" to consider both linear and non-linear transforms and assess potential benefits of RF-DNA fingerprinting when operating in multipath environments.

Section 2.2.3 provides a detailed description of the GT and GWT implementations considered here [9, 59, 92], along with RF-DNA fingerprint generation improvements that were required to process complex 2D T-F data.

1.2.2 Device Classification. Numerous *classification* methods exist within the pattern recognition community, with some of the most popular including Fisher's Linear Discriminant (FLD), K-Nearest Neighbor (kNN), Support Vector Machine (SVM), and simple cross-correlation techniques [40, 57, 82, 88, 94, 95]. The RF-DNA fingerprinting research in [57, 71, 74–76, 81, 93, 94] used the Fisher-based MDA/ML classifier to perform Multiple Discriminant Analysis (MDA) feature selection followed by Maximum Likelihood (ML) device discrimination using previously unseen data. It is also important to note that specialized *classification* techniques have seen little advancement [57]. Therefore, if a more robust set of 2D T-F features (e.g., DT-$\mathbb{C}$WT, GT, GWT, etc.) is combined with a more powerful classifier, it is expected that *classification* performance will improve.

While performing favorably in works cited previously using various signals of interest, there are some inherent drawbacks to the MDA/ML classifier, including:

1. The dimensionality of the N_C-dimensional input feature set is reduced through projection to a lower $(N_C - 1)$-dimensional subspace with a goal of maximizing

inter-class separation and minimizing intra-class spread. Through MDA feature selection, inherent input information is discarded through projection and the ability to identify significant input features, i.e., those having greatest impact on class separation and *classification* accuracy, is inherently lost;

2. MDA feature selection is performed independently of subsequent ML *classification*. This can lead to an undesirable effect of decreased *classification* accuracy when using a reduced dimensional feature set relative to what may be achievable using a full-dimensional feature set [64];

3. For ML *classification*, there is either 1) knowledge of the statistical distribution of each class' inputs, or 2) an assumption made on the statistical distributions. Traditionally, this includes assuming each class' inputs are normally distributed with equal costs and uniform prior probabilities [57, 74–76, 81, 93, 94]. However, specific knowledge of the distribution of each class' inputs may be unknown and the assumed normal condition may be violated under practical conditions (i.e., burst-to-burst signal variation, channel conditions, operating environments, etc.);

4. It has been suggested that the success of machine learning approaches (e.g., MDA/ML *classification*) is adversely affected by factors such as noisy or unreliable data, or irrelevant or redundant information [42].

Given noted MDA/ML drawbacks, Air Force Institute of Technology (AFIT) researchers have recently considered two alternate classifiers, including: 1) an Artificial Neural Network (ANN)-based Generalized Relevance Learning Vector Quantization-Improved (GRLVQI) process [43, 64], and 2) a Learning From Signals (LFS) process that is being jointly developed with researchers from Oak Ridge National Laboratory (ORNL) researchers [14, 44, 46, 47]. While both methods inherently overcome all MDA/ML drawbacks to some extent, the ability of GRLVQI and LFS to support Dimension Reduction Analysis (DRA) provides the greatest benefit, i.e., these methods inherently provide a means for identifying and retaining a reduced subset of most

relevant features contained in the full-dimensional feature set. The goal is to find a DRA reduced-dimensional subset that maintains a given *classification* performance and minimizes required computational resources.

Given the relative maturity of GRLVQI, it was adopted under this research as the process of choice for increasing classifier power. The increased "power" of this classifier rests not only in the potential for improving overall *classification* performance, but also in the fact that it provides a mechanism for determining which input features are most significant–a key deficiency of the MDA/ML classifier. Specific advantages of GRLVQI relative to MDA/ML drawbacks include [43, 64]:

1. Most importantly, a relevance ranking is assigned to each feature comprising an input RF-DNA fingerprint–a direct measure relating input feature significance to the overall *classification* decision.
2. Feature selection is performed in conjunction with *classification*.
3. No inherent assumption nor actual knowledge required on input data distribution (i.e., Gaussian, Rayleigh, etc.).
4. Processing is well-suited for cases where the number of input features may be inconsistent across classes, or where the inputs are comprised of noisy or inconsistent data.

Additional details on GRLVQI processing are provided in Section 2.3.2 and Section 3.3.2. Comparative *classification* performance results using RF-DNA based on traditional 1D TD and 1D SD features, as well as features based on joint 2D T-F responses are presented in Chapter IV.

1.2.3 Device ID Verification. Traditionally, RF-DNA fingerprint research has predominantly focused on device *classification* (a one-to-many looks "most like" assessment) [44, 47, 57, 74–76, 81, 93, 94]. In this case, the network "air monitor" would perform a "one-to-many" comparison to determine an *unknown* device's identity. This is done by comparing the current "challenge" RF-DNA from the *unknown* device to

the reference models stored for each of the *known* authorized network devices. Traditionally, in device *classification* the *unknown* device's "challenge" fingerprints will be assigned, by the classifier, as belonging to one of the known classes. This assignment is made regardless of whether or not the "challenge" RF-DNA originated from an authorized (i.e., reference model on hand) or *unknown* (i.e., no stored reference model) device. This leads to a final *classification* decision being made based upon a "best-match" criteria, where the best-match may actually be a poor match. Also, this "one-to-many" comparison may not be practical in all applications, including those where the air monitor supports a network comprised of a large number of devices and timely, accurate authentication is required. The challenge becomes even greater when considering networks where users enter and leave frequently or randomly (e.g., public WiFi hot spots, cellular-based networks, etc.).

This research adopted the *verification* procedures used in [19, 20] for unintentional emissions from electronic devices and applies them to intentional emissions from wireless devices to perform device ID *verification* (a one-to-one looks "how much like" assessment). This process involves a "one-to-one" comparison of the device's current RF-DNA fingerprint with a stored reference model associated with that device's digitally *claimed* bit-level identity; common digital identifiers include the Medium Access Control (MAC) address, Electronic Serial Number (ESN), International Mobile Equipment Identity (IMEI) number and the Subscriber Identity Module (SIM) number. As commonly done in network applications, *verification* results in [19, 20] and Chapter IV. results here are presented using Receiver Operating Characteristic (ROC) curves and corresponding Equal Error Rate (EER) to characterize device ID *verification* capability, with EER being the point at which False Reject Rate (FRR) equals False Accept Rate (FAR) [24, 53]. A more detailed description of device ID *verification* is presented in Section 2.4 and Section 3.5.

1.3 Research Contributions

Table 1.1 provides a summary of the technical areas identified in the previous sections, along with a relational mapping between "Previous Work" (pre-existing knowledge base) and contributions of the "Current Research" (knowledge base expansions) that are presented in this dissertation.

Table 1.1: Relational mapping between *Technical Areas* in *Previous* related work and *Current* research contributions. The × symbol denotes areas addressed.

Technical Area	Previous Work		Current Research	
	Addressed	Ref #	Addressed	Ref #
TD Fingerprinting	×	[23, 41, 56, 57] [81, 82, 93, 94]	×	[74–76]
SD Fingerprinting	×	[94]	×	[76]
DT-ℂWT Fingerprinting	×	[56–58]		
GT/GWT Fingerprinting			×	[45, 71–73, 76]
Signal Type/Modulation				
802.11/OFDM	×	[56–58, 94]	×	[45, 73]
GSM/GMSK	×	[93]	×	[74, 75]
802.16e/OFDMA	×	[94]	×	[71, 73, 76]
Device Classification				
GRLVQI	×	[56, 57]	×	[45, 72, 73]
LFS	×	[12–14, 44, 46, 47]	×	[45]
Dimension Reduction Analysis (DRA)				
GRLVQI	×	[56, 57]	×	[45, 72, 73]
LFS	×	[45]		
Device ID Verification				
Electronic Components	×	[19, 20]		
Authorized Wireless Devices			×	[72, 73]
Rogue Wireless Devices			×	[72, 73]

1.4 Document Organization

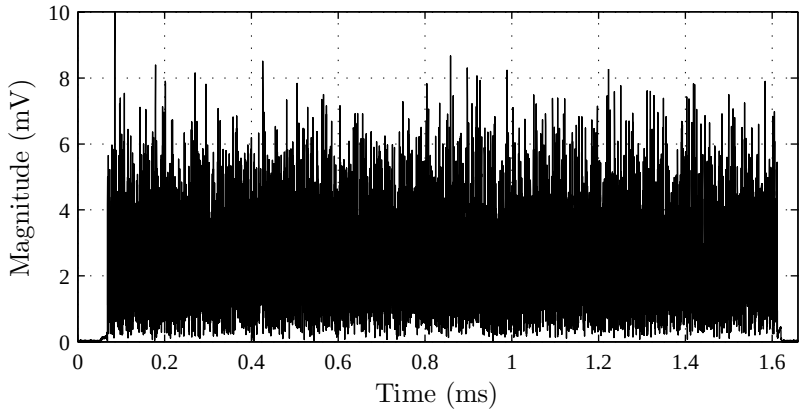
This document is organized as follows. Chapter II provides details on technical topics and literature related to OFDM-based WiMAX and WiFi signal implementation, RF signal collection, post-collection processing, RF-DNA fingerprinting, device *classification*, and device ID verification. Chapter III outlines the methodology used during the research to collect, process, generate fingerprints, and subsequently identify and/or verify IEEE 802.16e WiMAX and 802.11a WiFi devices. Chapter IV presents TD, SD, GT, and GWT device *classification* performance for the MDA/ML and GR-LVQI classifiers, as well as authorized and "rogue" device verification performance for the investigated signal types. Lastly, concluding comments and envisioned future research activity is presented in Chapter V.

II. Background

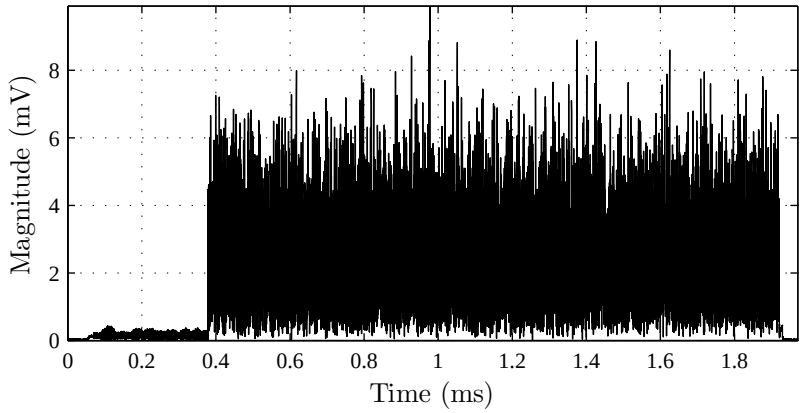
THIS chapter provides a summary of necessary technical concepts used in developing the research methodology presented in Chapter III, as well as generation of results presented in Chapter IV. Section 2.1 provides a description of the signals of interest which include IEEE compliant Wireless Fidelity (WiFi) and Worldwide Interoperability for Microwave Access (WiMAX) signals. Section 2.2 provides a description of RF-DNA fingerprint generation based on three specific responses, including 1D Time Domain (TD), 1D Spectral Domain (SD), and 2D joint (T-F) domain. Device *classification* using Multiple Discriminant Analysis/Maximum Likelihood (MDA/ML) and Generalized Relevance Learning Vector Quantization-Improved (GRLVQI) processes is presented in Section 2.3. The chapter concludes with Section 2.4 which describes the device ID *verification* process.

2.1 Signals of Interest

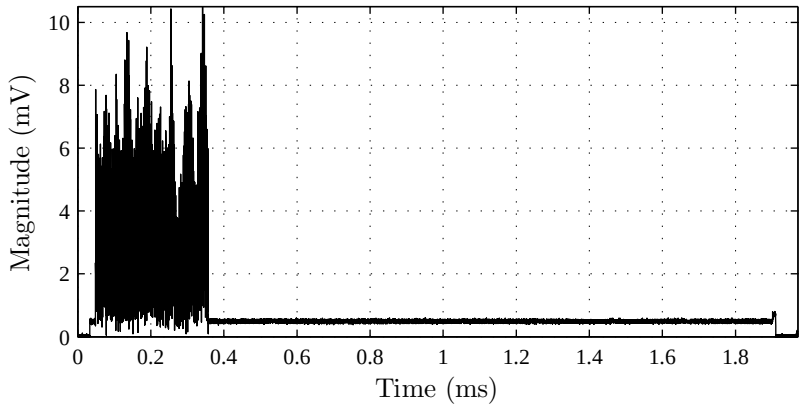
2.1.1 IEEE 802.16e WiMAX. An Alvarion BreezeMAX Extreme 5000 IEEE 802.16e WiMAX network using 60/40 Time Division Duplexing (TDD) was used for experimental demonstration. The first 60% of the T_F=5 ms TDD frame was allocated for Base Transciever Station (BTS) Down-Link (DL) transmission and the remaining 40% allocated for Mobile Subscriber (MS) Up-Link (UL) transmission [7]. The RF channel occupied a bandwidth of W_{Ch}=5 MHz centered at f_c=5475 MHz. Figure 2.1 presents magnitude plots for three distinct UL sub-frame responses that were observed during experimentation. As indicated, these are designated as *Data-Only*, *Range-Plus-Data*, and *Range-Only* mode responses [76]. These MS "operating modes" were not apparent in any Alvarion or supplemental documentation. When an MS transmits in the *Range-Plus-Data* or *Range-Only* modes, the ranging portion of the UL subframe is used for intial network setup, synchronization, BTS-to-BTS handover, resolution of bandwidth contention, as well as timing and frequency offset calculation [22, 50, 52]. All subsequent discussion as well as results presented in Chapter IV are based upon the tested MS operating in the *Range-Only* mode.



(a) MS *Data Only* sub-frame response.



(b) MS *Range-Plus-Data* sub-frame response.



(c) MS *Range Only* sub-frame response.

Figure 2.1: Three distinct UL sub-frame magnitude responses for "operating modes" of BreezeMAX 802.16e WiMAX MS transmissions [76].

Unlike previously investigated GSM and 802.11 signals [57, 58, 74, 75, 93], the collected mobile 802.16e WiMAX MS signals lack a distinct portion of the modulated waveform that remains consistent across all devices. However, all of the observed MS responses contained a device power up bias that spanned the UL sub-frame. This power up bias is most apparent in Fig. 2.1(c) and is expanded upon in Fig. 2.2. It is believed that the bias is incorporated by design to stabilize electronic component response and mitigate adverse peak-to-average power ratio effects that frequently occur in OFDM. An approximate 14.0 μs interval (2.0 μs to 16.0 μs) of the UL sub-frame response is designated here as the "near-transient" response. This "near-transient" response in Fig. 2.2 has thus far resulted in the most useful RF-DNA for WiMAX MS device *classification* and *verification* [71, 76].

2.1.2 IEEE 802.11a WiFi. IEEE 802.11a WiFi is an OFDM signal comprised of N_O=52 sub-carriers with a channel bandwidth of W_{Ch}=16.6 MHz centered at f_c=5745.2 MHz [51]. The 802.11a signal specification requires that each RF transmission include a distinctive preamble at the beginning. This distinct preamble is comprised of 10 short and 2 long training sequences. Networked devices use these sequences to assist in diversity selection, timing and frequency acquisition, and channel

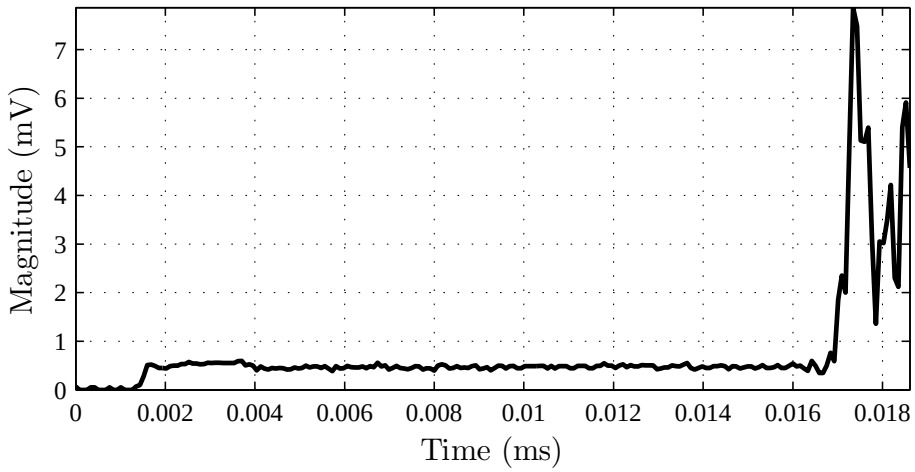


Figure 2.2: Expanded view of "near-transient" region of *Range-Only* magnitude response, of Fig. 2.1(c), showing the device power up bias present within the UL sub-frame [76].

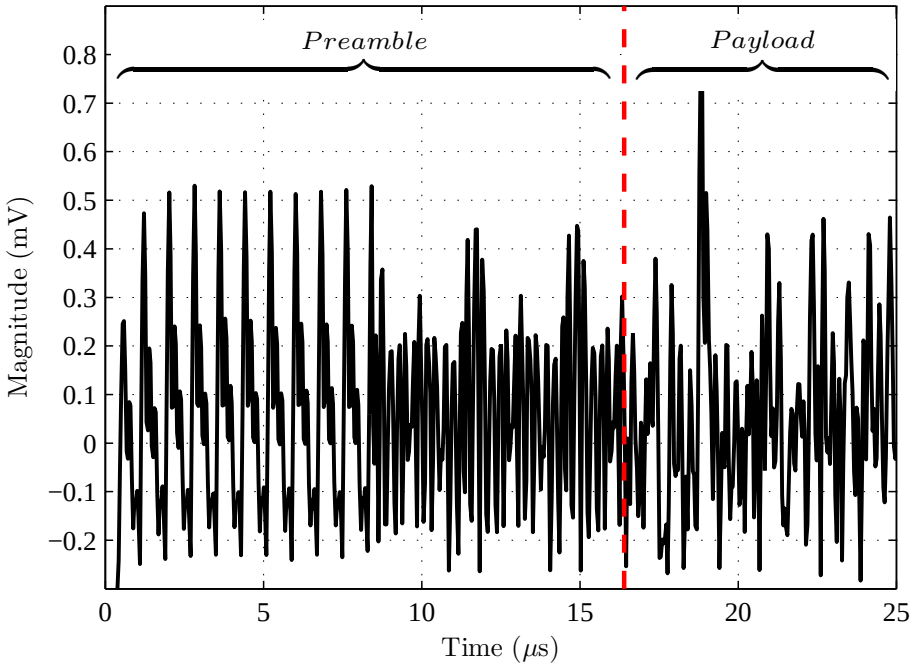


Figure 2.3: First 25 μs of an 802.11a WiFi burst (major portion of payload omitted). The preamble spans the first 16.5 μs [73].

estimation [51]. In this work, the signals used for experimental demonstration were collected from two laptops using Cisco AIR-CB21G-A-K9 WiFi cards operating as a peer-to-peer Ad hoc wireless network. Figure 2.3 illustrates the preamble, comprising the first 16.0 μs, of a 802.11a WiFi transmission from which RF-DNA fingerprints are extracted for subsequent device discrimination.

2.2 RF-DNA Fingerprinting

This work investigates the application of RF-DNA fingerprinting using features based on 1D Time Domain (TD), 1D Spectral Domain (SD), and 2D joint Time-Frequency (T-F) responses.

2.2.1 1D Time Domain (TD). As in [44,47,74–76,81,94], this work used RF-DNA fingerprints extracted from instantaneous TD amplitude, phase, and frequency responses. RF-DNA fingerprints ($\mathbf{f}_{TD}$) are generated from N_s samples extracted from the complex signal $s(n) = s_I(n) + js_Q(n)$. For consistency with [74–76, 81, 94], the

TD RF-DNA fingerprints are generated from the centered (denoted with subscript c) and normalized (denoted with over bar) amplitude $\{\bar{a}_c(n){:}n{=}1,\ldots,N_s\}$, phase $\{\bar{\phi}_c(n){:}n{=}1,\ldots,N_s\}$, and frequency $\{\bar{f}_c(n){:}n{=}1,\ldots,N_s\}$ sequences. The TD feature sequences are given by,

$$a(n) = \sqrt{s_I^2(n) + s_Q^2(n)}, \tag{2.1}$$

$$\phi(n) = \tan^{-1}\left[\frac{s_Q(n)}{s_I(n)}\right] \text{ , for } s_I(n) \neq 0, \tag{2.2}$$

$$f(n) = \frac{1}{2\pi}\left[\frac{d\phi(n)}{dn}\right] \text{ .} \tag{2.3}$$

Subsequent centering and normalization of the TD feature sequences is achieved by

$$\bar{a}_c(n) = \frac{a(n) - \mu_a}{\max\limits_n\{a_c(n)\}} \text{ ,} \tag{2.4}$$

$$\bar{\phi}_c(n) = \frac{\phi(n) - \mu_\phi}{\max\limits_n\{\phi_c(n)\}} \text{ ,} \tag{2.5}$$

$$\bar{f}_c(n) = \frac{f(n) - \mu_f}{\max\limits_n\{f_c(n)\}} \text{ ,} \tag{2.6}$$

where $n{=}1,\ldots,N_s$, μ_a, μ_ϕ and μ_f are the amplitude, phase, and frequency means calculated across N_s samples, and $max\{\cdot\}$ denotes the maximum of each feature sequence's centered magnitude.

As shown in Figure 2.4, an RF-DNA fingerprint ($\mathbf{f}_{TD}$) is generated by dividing each of the TD sequences into N_R equal length, sequential subregions such that N_s/N_R is an integer. Features are generated by calculating statistics: standard deviation (σ), variance (σ^2), skewness (γ), and/or kurtosis (κ), over each of the N_R subregions, as well as the $N_R + 1$ subregion which spans the entire length of a TD sequence. The calculated statistics, for each of the selected subregions, are arranged as follows:

$$\mathbf{f}_{R_i} = [\sigma_{R_i}, \sigma_{R_i}^2, \gamma_{R_i}, \kappa_{R_i}]_{1\times 4} \text{ ,} \tag{2.7}$$

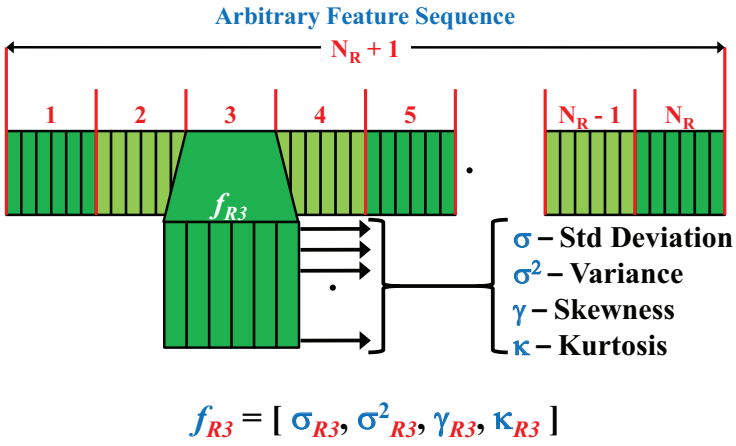


Figure 2.4: Regional fingerprint generation for N_R+1 total regions using the centered and normalized feature sequences [94].

where $i = 1, 2, \ldots, N_R$+1. A composite fingerprint is formed by concatenating the statistical features calculated to form (2.7) with one another for a selected TD sequence as follows [94],

$$\mathbf{f}^{\delta} = \left[\mathbf{f}_{R_1} \vdots \mathbf{f}_{R_2} \vdots \mathbf{f}_{R_3} \cdots \mathbf{f}_{R_{N_R+1}} \right]_{1\times 4(N_R+1)}, \tag{2.8}$$

where the superscript δ denotes a specific TD sequence, i.e., $\{\bar{a}_c(n)\}$, $\{\bar{\phi}_c(n)\}$ or $\{\bar{f}_c(n)\}$. Due to the use of multiple TD sequences in the generation of TD RF-DNA fingerprints, the composite fingerprints from (2.8) are concatenated to compose $\mathbf{f}_{TD}$ as follows:

$$\mathbf{f}_{TD} = \left[\mathbf{f}^{a} \vdots \mathbf{f}^{\phi} \vdots \mathbf{f}^{f} \right]_{1\times 4(N_R+1)\times 3}. \tag{2.9}$$

Therefore, $\mathbf{f}_{TD}$ contains a total of N_f^{TD} = (# of Features) × (# of Statistics) × (# of Regions + 1) elements.

2.2.2 1D Spectral Domain (SD). RF-DNA fingerprinting is performed using SD features generated as in [94] and based upon the TD methods outlined in Section 2.2.1. SD RF-DNA fingerprints ($\mathbf{f}_{SD}$) are generated using the power-normalized Power Spectral Density (PSD) of the complex signal sequence $\{s(n)\}$ [94]. The Discrete Fourier Transform (DFT) is used in calculating the desired PSD feature sequence

$\{\bar{p}(k)\}$ as follows [70],

$$S(k) = \frac{1}{N_s} \sum_{n=1}^{N_s} s(n) e^{-j\Phi(N_s,n,k)}, \tag{2.10}$$

$$\Phi(N_s, n, k) = \left(\frac{2\pi}{N_s}\right)(n-1)(k-1), \tag{2.11}$$

where k=0.1, ..., N_s. To obtain the desired power-normalized PSD sequence $\{\bar{p}(k)\}$, (2.10) is divided by the signal's average power,

$$\bar{p}(k) = \frac{1}{P_s}|S(k)|^2, \tag{2.12}$$

where P_s is given by,

$$P_s = \frac{1}{N_s} \sum_{n=1}^{N_s} s(n)s(n)^*, \tag{2.13}$$

and $*$ denotes complex conjugate. The PSD is normalized to diminish potential collection process effects that may bias the *classification* results. As in [23, 76, 81, 82, 94], the DC (k=0) and redundant $\left(N_s/2+1, N_s/2+2, \ldots, N_s\right)$ terms of $\{\bar{p}(k)\}$ are removed prior to statistical fingerprint generation. As with the TD process, outlined in Section 2.2.1, statistics are calculated over N_R contiguous sub-regions within the power-normalized PSD. Each SD RF-DNA fingerprint ($\mathbf{f}_{SD}$) is formed by grouping the statistics as in (2.7) and subsequent concatenation to generate SD RF-DNA fingerprints of the form,

$$\mathbf{f}_{SD} = \left[\mathbf{f}_{R_1} \vdots \mathbf{f}_{R_2} \vdots \mathbf{f}_{R_3} \ \cdots \ \mathbf{f}_{R_{N_R+1}} \right]_{1\times 4(N_R+1)}. \tag{2.14}$$

The process in (2.14) results in $\mathbf{f}_{SD}$ being comprised of a total of N_f^{SD} = (# of Statistics)$\times$ (# of Regions + 1) elements.

2.2.3 2D Joint Time-Frequency (T-F) Domain. In a majority of previous related work, RF-DNA fingerprints were predominantly extracted from 1D TD and SD responses [57, 58, 74, 75, 94], with Dual-Tree $\mathbb{C}$omplex Wavelet Transform (DT-$\mathbb{C}$WT) coefficients being AFIT's first application of joint 2D features [56, 57]. The

use of DT-ℂWT coefficients is consistent with conclusions in [9] indicating that the use of momentary and/or time localized energy as a function of frequency can be effective for describing signals. This motivated the use of 2D T-F localization using the Discrete Gabor Transform (DGT) which is calculated as follows [9],

$$\mathbf{G}_{mk} = \sum_{n=1}^{MN_\Delta} s(n)W^*(n - mN_\Delta)\exp^{-j2\pi kn/K_G}, \tag{2.15}$$

where $\mathbf{G}_{mk}$ are the Gabor coefficients, $s(n)$=$s(n+lMN_\Delta)$ is the periodic input signal, $W(n) = W(n+lMN_\Delta)$ is the periodic analysis window, N_Δ is the number of samples shifted, m=$1, 2, \ldots, M$ for M total shifts, and k=$0, 1, \ldots, K_G-1$ for $K_G \geq N_\Delta$ and $mod(MN_\Delta, K_G)$=0 satisfied [76]. In the case where K_G=N_Δ, the Gabor transformation represents *critical sampling*. *Oversampling* occurs when $K_G > N_\Delta$ and is desirable when processing noisy data [9, 35, 92, 97]. Therefore, oversampling was deemed appropriate for this research given collected signal of interest responses are noisy; thus, enabling a more reliable analysis with varying SNR. As in [9], the DGT was implemented using a Gaussian analysis window $W(n)$.

The GT is combined with the Wigner-Ville Distribution (WVD) to form the Gabor-Wigner Transform (GWT) [68]. This combination takes advantage of the GTs lack of cross-terms and faster computation as well as the higher clarity of the WVD. While somewhat arbitrary in terms of exponential weighting, and without regard for optimizing performance, the GWT is computed here using [68],

$$\mathbf{GW}_{mk} = \mathbf{G}_{mk}^{2.6}\mathbf{V}_{mk}^{0.6}, \tag{2.16}$$

where $\mathbf{V}_{mk}$ is the Discrete Pseudo Wigner Distribution (DPWD) given by [18],

$$\mathbf{V}_{mk} = \sum_{n=-(K_G/2-1)}^{K_G/2-1} h(n)exp^{-j2\pi kn/K_G}, \tag{2.17}$$

$$h(n) = w(n)w^*(n)s(m+n)s^*(m-n), \tag{2.18}$$

and Hamming window function $w(n)$ is implemented as in [18]. RF-DNA fingerprints are generated from the *normalized* magnitude-squared Gabor and Gabor-Wigner coefficients $|\mathbf{G}_{mk}|^2$ and $|\mathbf{GW}_{mk}|^2$, respectively. The magnitude-squared coefficients are *normalized* by,

$$\overline{|\mathbf{A}_{mk}|^2} = \frac{|\mathbf{A}_{mk}|^2 - min\{\ |\mathbf{A}_{mk}|^2\ \}}{max\{\ |\mathbf{A}_{mk}|^2 - min\{\ |\mathbf{A}_{mk}|^2\ \}\ \}}\ . \tag{2.19}$$

where $\mathbf{A}_{mk}$ are the coefficients of the selected T-F transform.

As shown in Fig. 2.5, the resulting T-F surface is divided into $N_T \times N_F$ 2-dimensional subregions (patches), vectorized, and statistics calculated (standard deviation, variance, skewness, and kurtosis). The dimensions of each $N_T \times N_F$ patch are selected to ensure a minimum of N_{TF}=15 entries are used for statistical calculation. Similar to TD and SD RF-DNA fingerprint generation, statistics calculated over the entire T-F surface are included and represent the $N_R + 1$ subregion.

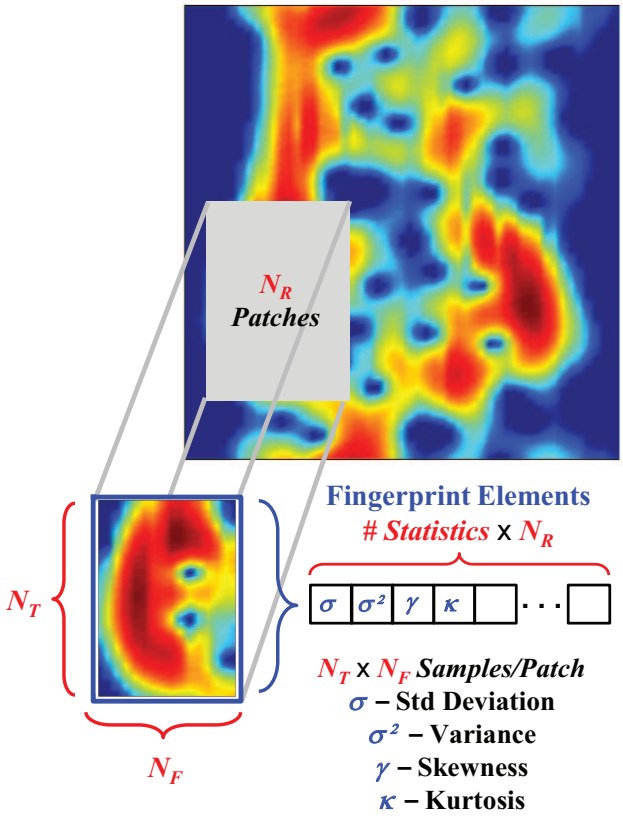


Figure 2.5: Gabor-based RF-DNA fingerprint generation using $N_T \times N_F$ 2D T-F patches of centered and normalized magnitude-squared GT and GWT coefficients [76].

2.3 Device Classification

2.3.1 MDA/ML Processing. As in [20, 74–76, 81, 82, 94], MDA/ML is used to perform feature selection and device *classification* (a one-to-many "best match" assessment). The goal of MDA is to reduce feature dimensionality while improving class separability. MDA is an extension of Fisher's Linear Discriminant Analysis (LDA) from a two-class case to the N_C-class case, where N_C is the total number of classes/devices. MDA is a linear operation that projects the samples (i.e., the RF-DNA fingerprints) to a (N_C-1)-dimensional subspace without reducing the power of class separability [87]. The MDA projection maximizes inter-class distances while minimizing intra-class spread.

In MDA, the between (inter-) ($\mathbf{S}_b$) and within (intra-) ($\mathbf{S}_\omega$) class scatter matrices are computed [87]:

$$\mathbf{S}_b = \sum_{i=1}^{C} P_i \mathbf{\Sigma}_i, \tag{2.20}$$

$$\mathbf{S}_\omega = \sum_{i=1}^{C} P_i (\mu_i - \mu_0)(\mu_i - \mu_0)^T, \tag{2.21}$$

where $\mathbf{\Sigma}_i$ and P_i are the covariance matrix and prior probability of class c_i, respectively. Individual RF-DNA fingerprints are projected into the lower (N_C-1)-dimensional subspace by:

$$\mathbf{f}_i^{\mathbf{W}} = \mathbf{W}^T \mathbf{f}, \tag{2.22}$$

where $\mathbf{W}$ is the projection matrix formed from the (N_C-1) eigenvectors of $\mathbf{S}_\omega^{-1}\mathbf{S}_b$. It is through the formation of the projection matrix $\mathbf{W}$ that results in the optimal ratio between the inter-class distances and intra-class variances [87]. Figure 2.6 provides a representative illustration of two possible MDA projection matrices. In this case, projection matrix $\mathbf{W}_1$ provides "best" case class separation performance.

For each class, a total of N_τ training fingerprints are projected (denoted by the superscript $\mathbf{W}$) during the MDA training process to form the projected training

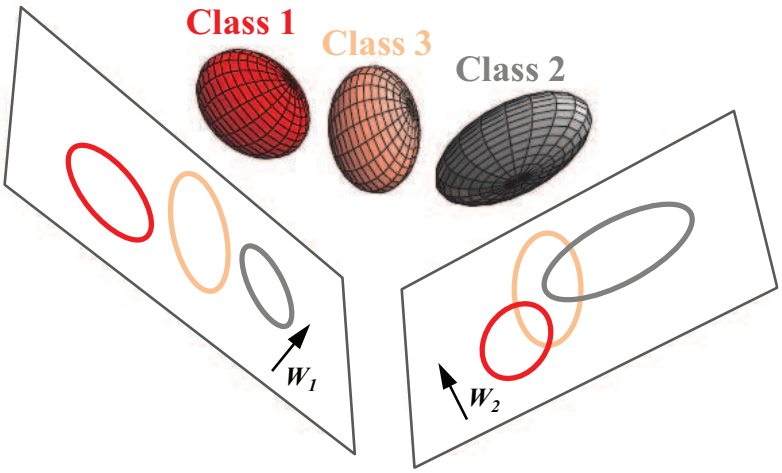


Figure 2.6: Representative MDA projection from N_C=3 class inputs to two possible N_C-1=2D subspaces. [30].

matrix $\mathbf{f}^{\mathbf{W}}$ as follows:

$$\mathbf{f}^{\mathbf{W}} = \left[\mathbf{f}_1^{\mathbf{W}}, \mathbf{f}_2^{\mathbf{W}}, \cdots, \mathbf{f}_{N_\tau}^{\mathbf{W}}\right]^T_{N_\tau \times (C-1)}. \tag{2.23}$$

The mean vector $\widehat{\mu}_i^{\mathbf{W}}$ and covariance matrix $\widehat{\mathbf{\Sigma}}_i^{\mathbf{W}}$ are estimated and stored for each class' projected training fingerprints. A multi-variate Gaussian distribution, computed using the pooled covariance matrix $\widehat{\mathbf{\Sigma}}_P^{\mathbf{W}}$ and appropriate estimated mean vector $\widehat{\mu}_i^{\mathbf{W}}$, is fitted to each class' training samples to form the reference models. These reference models are used to estimate the similarity measure/likelihood values of the given fingerprint $\hat{\mathbf{f}}$ [87]:

$$P(\hat{\mathbf{f}}|c_i) = \frac{1}{(2\pi)^{(C-1)/2}\,\det(\widehat{\mathbf{\Sigma}}_P^{\mathbf{W}})^{1/2}} \cdot \exp\left(\mathcal{F}_e\right), \tag{2.24}$$

where,

$$\mathcal{F}_e = -\frac{1}{2}(\hat{\mathbf{f}} - \widehat{\mu}_i)^T(\widehat{\mathbf{\Sigma}}_P^{\mathbf{W}})^{-1}(\hat{\mathbf{f}} - \widehat{\mu}_i). \tag{2.25}$$

Average percent correct device *classification* is calculated as the percentage of the time the classifier correctly assigns an observed RF-DNA fingerprint to its true class over all trials. The pooled covariance matrix $\widehat{\mathbf{\Sigma}}_P^{\mathbf{W}}$, used in subsequent generation of each

class' reference model, is calculated from the individual estimated class covariances $\widehat{\mathbf{\Sigma}}_i^{\mathbf{W}}$ as follows,

$$\widehat{\mathbf{\Sigma}}_P^{\mathbf{W}} = \frac{1}{N_\tau - N_C} \sum_{i=1}^{N_C} \widehat{\mathbf{\Sigma}}_i^{\mathbf{W}}, \tag{2.26}$$

where N_C is the total number of classes (devices).

A device's identity is determined through the comparison of its *unknown* RF-DNA fingerprint with each reference model that has been fit to each of the N_C training sets following feature selection. A *classification* decision is made by computing a similarity measure between the unknown RF-DNA fingerprint and each of the N_C known reference templates and assigning it to the class that results in the best match. As in [20], this work uses the Bayesian posterior probability, under the assumptions of uniform costs and equal priors, as the similarity measure. This approach optimally minimizes the *classification* error probability [87]. In the case of N_C devices, an *unknown* device's RF-DNA fingerprint $\hat{\mathbf{f}}$ is assigned to class c_i if:

$$P(c_i|\hat{\mathbf{f}}) > P(c_j|\hat{\mathbf{f}}) \; \forall j \neq i, \tag{2.27}$$

where $i \in \{1, 2, \ldots, N_C\}$ and $P(c_i|\hat{\mathbf{f}})$ is the conditional posterior probability that $\hat{\mathbf{f}}$ belongs to class c_i. Applying Bayes' Rule, the conditional probability is computed as [62]:

$$P(c_i|\hat{\mathbf{f}}) = \frac{P(\hat{\mathbf{f}}|c_i)P(c_i)}{P(\hat{\mathbf{f}})}. \tag{2.28}$$

Due to the assumption of equal prior probabilities ($P(c_i) = {}^1/_{N_C}$) for all classes, $P(c_i)$ can be neglected when evaluating (2.28). Since the conditional probability is being calculated for a given fingerprint $\hat{\mathbf{f}}$, the denominator remains constant across all c_i and can be neglected as well. This reduces the decision criteria in (2.28) to maximizing the likelihood for $P(\hat{\mathbf{f}}|c_i)$ for all c_i.

2.3.2 GRLVQI Processing. GRLVQI possesses several inherent advantages over MDA/ML-based *classification* and is introduced here for RF-DNA fingerprinting given that [43, 64]:

1. There is no inherent assumption nor actual knowledge required on input data distribution (Gaussian, Rayleigh, etc.).
2. Feature selection is performed in conjunction with *classification*.
3. Processing is well-suited for cases where the number of inputs may be inconsistent across classes or where the inputs are comprised of noisy or inconsistent data.
4. A relevance ranking is assigned to each feature comprising an input RF-DNA fingerprint.

This last advantage was the most important for this research in that a direct measure relating input feature significance to the overall *classification* decision facilitates Dimensionality Reduction Analysis (DRA).

For GRLVQI classifier training (model development), a predefined number of prototype vectors (N_P), each comprised of N_f features, are assigned to represent each of the N_C classes/devices. The collection of all prototype vectors ($\mathbf{p}^n$) is used to form matrix $\mathbf{P}$ of dimension $(N_C \cdot N_P) \times N_f$ with the goal of defining *classification* boundaries that minimize the Bayes risk. The Bayes risk is minimized by *differentially shifting* the best *In-Class* $\mathbf{p}^I$ and *Out-of-Class* $\mathbf{p}^O$ prototype vectors by some distortion d_λ^n computed via [43],

$$d_\lambda^n = \sum_{i=1}^{N_f} \lambda_i (\mathbf{f}_i^m - \mathbf{p}_i^n)^2, \tag{2.29}$$

where $n = 1, 2, \ldots, N_P$, N_f is the number of features comprising an RF-DNA fingerprint, $\mathbf{f}^m$ is a randomly selected input fingerprint, $\mathbf{p}^n \in \mathbf{P}$, and λ_i is the relevance (importance weighting) of the i^{th} feature satisfying $||\boldsymbol{\lambda}||_1 = 1$ [43] with $\lambda_i \geq 0 \; \forall \; i \in \{1, \ldots, N_f\}$. At the beginning of the classifier training process, λ_i is randomly initiated. The work

in [64] introduces a bias parameter B^n that is adapted from [26] to minimize utilization of poor prototype vectors. The resultant distortion is given by

$$d^n_{Bias} = d^n_\lambda - B^n \ , \tag{2.30}$$

$$B^n = \psi \left(\frac{1}{N_P} - F^n_{\text{old}} \right) \ , \tag{2.31}$$

where ψ is selected by the user to control the amount of bias that is applied to the distortion and F^n_{old} is the frequency at which a prototype vector is selected as the "best" prototype vector (i.e., it has the smallest d^n_{Bias} to $\mathbf{f}^m$).

The best in-class prototype vector $\mathbf{p}^I$ is the $\mathbf{p}^n$, with the *same* class label as $\mathbf{f}^m$, for which d^n_{Bias} is the smallest. The in-class prototype vector distortion d^I=d^n_{Bias} (i.e., the distortion value that resulted in selection of $\mathbf{p}^I$). The best out-of-class prototype vector $\mathbf{p}^O$ is the $\mathbf{p}^n$, with a class label that is *different* than that of $\mathbf{f}^m$, for which d^n_{Bias} is the smallest. Thus, the out-of-class prototype vector distortion d^O=d^n_{Bias}. The prototypes are updated following selection of the best in-class and out-of-class prototype vectors by [43],

$$\mathbf{p}^I(t+1) = \mathbf{p}^I(t) + \frac{4\alpha^I(t) f'|_{\mu(\mathbf{f}^m),\tau} d^O}{(d^I + d^O)^2} \mathbf{\Lambda}(\mathbf{f}^m - \mathbf{p}^I(t)), \tag{2.32}$$

$$\mathbf{p}^O(t+1) = \mathbf{p}^O(t) + \frac{4\alpha^O(t) f'|_{\mu(\mathbf{f}^m),\tau} d^I}{(d^I + d^O)^2} \mathbf{\Lambda}(\mathbf{f}^m - \mathbf{p}^O(t)), \tag{2.33}$$

where $\mathbf{\Lambda}_{i,i} = \lambda_i$, α^I and α^O are the learn rates for the in-class and out-of-class prototypes, τ is a time decay term [64], and $f'|_{\mu(\mathbf{f}^m),\tau}$ is the first derivative of the sigmoid loss function:

$$f(\mu(\mathbf{f}^m), \tau) = \frac{1}{1 + e^{-\tau\mu(\mathbf{f}^m)}}, \tag{2.34}$$

$$\mu(\mathbf{f}^m) = \left(\frac{d^I - d^O}{d^I + d^O} \right), \tag{2.35}$$

where $\mu(\mathbf{f}^m)$ is the misclassification measure [77]. If $\mu(\mathbf{f}^m)$<0, with $\mu(\mathbf{f}^m)$=−1 being perfect *classification*, then a correct *classification* occurs. Conversely, a misclassifi-

cation occurs if $\mu(\mathbf{f}^m) \geq 0$ [77]. GRLVQI implements a conditional update rule in an effort to minimize potential divergence of the prototype vectors. Under this rule, both of the in-class and out-of-class winning prototype vectors are updated *only* if the input sample is misclassified; otherwise, only the in-class prototype vector is updated [64].

Following selection of the best in-class and out-of-class prototype vectors, the learn rates α^I and α^O are adjusted and the relevances updated using [43]

$$\Delta\lambda_i = -\frac{2\alpha(t)^{\boldsymbol{\lambda}} f'|_{\mu(\mathbf{f}^m),\tau}\left[d^O(\mathbf{f}^m - \mathbf{p}^I)^2\right]}{(d^I + d^O)^2} + \frac{2\alpha(t)^{\boldsymbol{\lambda}} f'|_{\mu(\mathbf{f}^m),\tau}\left[d^I(\mathbf{f}^m - \mathbf{p}^O)^2\right]}{(d^I + d^O)^2} \ . \quad (2.36)$$

The process is iterated for a given number of iterations (N_I) or until other termination criteria are satisfied. Following termination, the prototype vectors representing the best model fit and associated $\boldsymbol{\lambda}$ are available for feature DRA. The corresponding "best" *Relevance Vector* is given by

$$\boldsymbol{\lambda}_B = [\lambda_1, \lambda_2, ..., \lambda_{N_f}] \ , \quad (2.37)$$

where a higher λ_i value for a given feature indicates that that feature has greater impact on *classification* performance.

Figure 2.7 illustrates GRLVQI *classification*, in which the distance between an *unknown* RF-DNA fingerprint ($\hat{\mathbf{f}}$) and each of the prototype vectors comprising the "best" model $\mathbf{P}_B$ is computed by (2.29). The *unknown* RF-DNA fingerprint ($\hat{\mathbf{f}}$) is subsequently assigned to class C_i by,

$$C_i : \underset{i,j}{\operatorname{argmin}} \left(d_{\lambda}^{p}(\mathbf{p}_{i,j}, \hat{\mathbf{f}}) \right) \ , \quad (2.38)$$

where $\mathbf{p}_{i,j} \in \mathbf{P}_B$, $i = 1, 2, \ldots, N_C$, and $j = 1, 2, \ldots, N_P$.

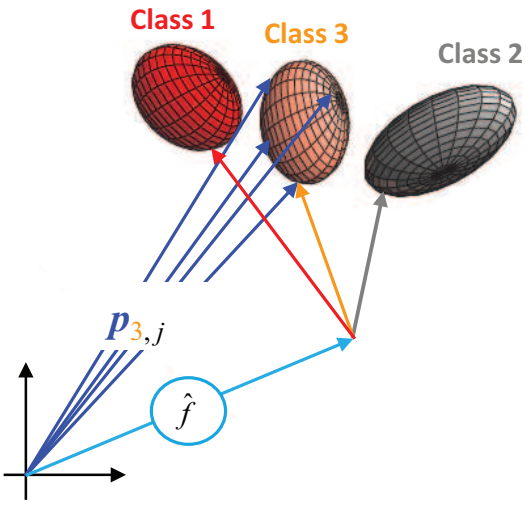


Figure 2.7: GRLVQI *classification* process with an *unknown* fingerprint ($\hat{\mathbf{f}}$) assigned to class C_i based upon minimum Euclidean Distance computed in (2.29) [73].

2.4 Device ID Verification

Unlike device *classification*, a one-to-many looks "most like" assessment whereby an unknown device's RF-DNA fingerprints are compared to each of the N_C reference models, device ID *verification* is a one-to-one looks "how much" assessment that enables authentication of a device's digitally claimed bit-level identity: Medium Access Control (MAC) address, Electronic Serial Number (ESN), International Mobile Equipment Identity (IMEI) number, or the Subscriber Identity Module (SIM) number. For this research, a device that falsely claims a digital identity that is different than its own, in order to gain unauthorized network access, is designated as a "rogue" device. In this case, the claimed identity is compared against the specific reference model associated with the true identity [20]. The resultant *verification* decision is binary, with the device's claimed identity declared authentic (rightly or wrongly) when the *verification* test statistic meets or exceeds a predetermined threshold. If the test statistic fails to meet the *verification* decision threshold, the device is deemed to be an impostor/impersonator and network access is denied.

As indicated in Table 2.1 and summarized below, there are two types of *verification* errors that can be made [20, 24, 53]:

1. *False Verification*: A rogue device's false claimed ID is deemed authentic and the device is granted network access–measured as False Verification Rate (FVR).
2. *False Reject*: An authorized device's true claimed ID is deemed rogue and the device is not granted network access–measured as False Reject Rate (FRR).

Table 2.1: Verification Outcomes & Rates.

	System Declaration (Rate)	
Actual	Authorized	Rogue
Authorized	True Verification (TVR)	False Reject (FRR)
Rogue	False Verification (FVR)	True Reject (TRR)

By varying the decision threshold t_v, system security can be increased to reduce false *verification* errors or decreased to reduce false reject errors. The Receiver Operating Characteristic (ROC) curve and corresponding Equal Error Rate (EER) are used to establish device *verification* capability [20, 24]. The ROC curve is created by plotting True Verification Rate (TVR) versus False Verification Rate (FVR) as the threshold value t_v is varied [24, 53]. The EER is defined as the point on the ROC curve at which the False Reject Rate (FRR = 1-TVR) equals the FVR. The EER is commonly used as a summary statistic for comparing *verification* performance across multiple systems; however, it may not represent the desired operating point in a fielded system. In general, a lower EER value indicates better *verification* performance for a given system [20, 24].

III. Research Methodology

THIS chapter describes the signal collection, detection, post-collection processing, *classification* and *verification* processes developed under this research, as based on work in [74] and illustrated in Fig. 3.1. Section 3.1 outlines the signal collection process which is performed using AFITs RF Signal Intercept and Collection System (RFSICS). Section 3.2 describes the post-collection processing which includes digital filtering, burst detection, and the addition of scaled, like-filtered Additive White Gaussian (AWGN) for varying the analysis SNR (SNR_A). This research considered two different *classification* processing techniques: Section 3.3.1 describes the Fisher-based Multiple Discriminant Analysis/Maximum Likelihood (MDA/ML) process and Section 3.3.2 describes the Artificial Neural Network (ANN)-based Generalized Relevance Learning Vector Quantization-Improved (GRLVQI) process. Device bit-level identification (ID) *verification* is described in Section 3.5.1 and Section 3.5.2 using reference models developed during the MDA/ML and GRLVQI classifier training processes, respectively.

3.1 Signal Collection

The signal collection process is illustrated in Fig. 3.1 and includes the use of an Agilent E3238S-based RFSICS having a fixed RF input filter bandwidth of W_{RF}=36.0 MHz that is tunable across the range of $f_{RF} \in [20.0\ MHz, 6.0\ GHz]$ [6]. The selected frequency band is down-converted to an Intermediate Frequency (IF) of f_{IF}=70 MHz and digitized by an N_b=12 bit Analog-to-Digital Converter (ADC) operating at a sampling rate of f_s=95 mega-samples-per-second (Msps). During analog-to-digital conversion, the IF signal is down-converted to baseband, digitally filtered, sub-sampled in accordance with Nyquist criteria, and subsequently stored as complex In-Phase (I) and Quadrature (Q) data. The devices under test and the RFSICS are co-located in an office building environment during all collections.

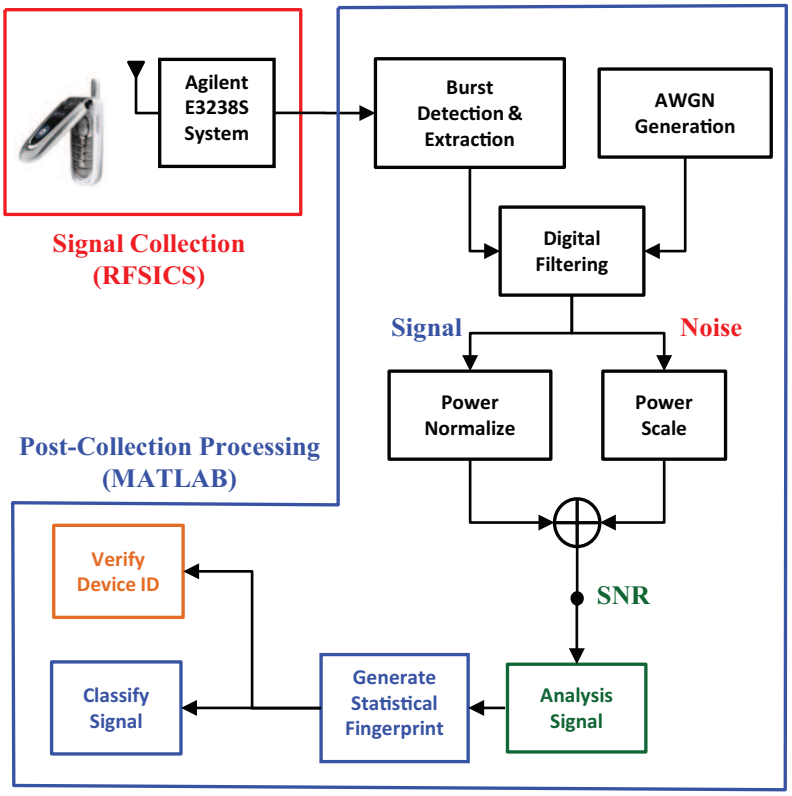


Figure 3.1: Signal collection and post-collection processing [74].

3.2 Post-Collection Processing

Following collection, down-conversion, and storage, the RFSICS signal file is converted to `Matlab`® format for post-collection processing, which included: 1) digital baseband filtering, 2) individual burst detection using Variance Trajectory (VT) based upon the work in [58], 3) detected burst removal from the collection record, and 4) noise power generation, scaling and addition to achieve the desired SNR_A and model the effects of differing channel conditions. For this work, the like-filtered AWGN was scaled to achieve the desired $SNR_A \in$[-3.0,27.0] dB and added directly to the collected $I-Q$ data. Given the relatively benign signal collection environment and correspondingly high collected SNR_c which was typically in the range of $SNR_c \in [30.0, 40.0]$ dB, the like-filtered AWGN was the dominant noise source.

Observation: While effective for development and proof-of-concept demonstration, the like-filtered AWGN SNR_A scaling process may not accurately reflect true SNR variation effects caused by non-Gaussian channel noise (e.g., Rayleigh, Chi, Chi-Squared, etc.).

3.2.1 Digital Filtering. Collected signal SNR is improved by applying digital filtering prior to burst detection. This filtering induces signal "coloration" effects that are representative of what actually occurs in realistic hardware processing. Table 3.1 provides the parameters used for implementing the lowpass Butterworth filters for the WiMAX and WiFi signals. For consistency with related signal modulation work, the filter parameters were selected to achieve a baseband bandwidth W_{BB} that is "slightly larger" than the signal bandwidth, [8].

Table 3.1: Digital Filter Parameters.

	Order (N_o)	Bandwidth (W_{BB})
WiMAX	6	2.5 MHz
WiFi	4	7.7 MHz

3.2.2 Burst Detection. Amplitude-based Variance Trajectory (VT) detection is used to locate and extract desired burst responses from the overall collection record. Elements of the VT sequence $\{VT_a(n)\}$ are generated from the instantaneous amplitude sequence $\{a(n)\}$, containing elements generated per equation (2.1), and are generated using,

$$VT_a(n) = |W_a(n) - W_a(n+1)|, \tag{3.1}$$

$$W_a(m) = \frac{1}{N_w} \sum_{n=1+(m-1)N_A}^{1+(m-1)N_A+N_w} [a(n) - \mu_w]^2,$$

where n=$1, 2, \ldots, L_w - 1,\ m$=$1, 2, \ldots,\ L_w, L_w$=$\lfloor (N_a - N_w)/N_s \rfloor + 1$, N_a is the total number of samples comprising $a(n)$, N_w is the window width and N_A is the number of samples the window advances between calculations. The sample mean μ_w is calculated

over consecutive subsequence of elements $\{a_w(n)\}$, taken from $\{a(n)\}$ and contained in the window [58].

3.2.3 Signal-to-Noise Ratio (SNR) Scaling. Following VT burst detection, the SNR of complex collected signals is on the order of $SNR_c \in [30.0, 40.0]$ dB. These high SNR_c levels allow the addition of power-scaled, like-filtered AWGN to generate analysis signals at the desired SNR_A. These signals facilitate analysis of RF-DNA fingerprint generation, feature selection, device *classification*, and *verification* under various degraded SNR conditions.

The average power (X) in an arbitrary complex sequence $\{x(k)\}$, k=1, 2, ..., K, is given by,

$$X = \frac{1}{K} \sum_{k=1}^{K} x(k)x^*(k), \tag{3.2}$$

where $x^*(k)$ denotes the complex conjugate of $x(k)$. Elements of the complex collected signal sequence $\{s_c(k)\}$ are comprised of two components,

$$s_c(k) = s_t(k) + n_b(k), \tag{3.3}$$

where $s_t(k)$ and $n_b(k)$ are elements of the transmitted complex signal and background noise sequences, respectively. Under the assumptions that 1) the $\{s_t(k)\}$ and $\{n_b(k)\}$ random sequences are independent, and 2) the $E[\{n_b(k)\}]$=0, the total average power S_c in K samples of $\{s_c(k)\}$ is given by,

$$S_c = S_t + N_b, \tag{3.4}$$

where S_t and N_b are calculated using (3.2) and given by,

$$S_t = \frac{1}{K} \sum_{k=1}^{K} s_t(k)s_t^*(k), \tag{3.5}$$

$$N_b = \frac{1}{K}\sum_{k=1}^{K} n_b(k)n_b^*(k). \tag{3.6}$$

Under the two previously stated assumptions, (3.5) and (3.6) can be used to calculate the collected signal SNR (in dB) as follows:

$$SNR_c^{\text{dB}} = 10 \times log_{10}\left(\frac{S_t}{N_b}\right). \tag{3.7}$$

Now accounting for the addition of zero mean, independent AWGN samples $n_A(k)$, elements of the desired analysis signal sequence $\{s_A(k)\}$ are generated using (3.3) and given by,

$$s_A(k) = s_t(k) + n_b(k) + n_A(k). \tag{3.8}$$

The desired analysis SNR_A of sequence $\{s_A(k)\}$ is achieved by scaling the average power in $\{n_A(k)\}$. The elements in $\{n_A(k)\}$ are first generated as independent complex AWGN samples such that $E[\{n_A(k)\}]$=0 (zero mean) and $E[\{n_A(k)^2\}]$=1 (unit variance). The complex noise samples are then digitally filtered using the same parameters used to filter the signal of interest (WiMAX or WiFi per Table 3.1 in Section 3.2.1). The like-filtered, complex noise samples are then multiplied by scale factor R_n to achieve the desired SNR_A, with power-scaling factor R_n calculated as,

$$R_n = \sqrt{10^{\frac{SNR_A^{dB}}{10}} \times S_t}. \tag{3.9}$$

Multiplying each filtered noise sample by R_n yields a total average AWGN power that is denoted here by P_G. Using this, the SNR_A (in dB) for the analysis signal given by (3.8) can be calculated using,

$$SNR_A^{\text{dB}} = 10 \times log_{10}\left(\frac{S_t}{N_b + P_G}\right) \ . \tag{3.10}$$

Given the range of actual collected $SNR_c \in [30.0, 40.0]$ dB, and the desired range of analysis $SNR_A \in$[-3.0,27.0] dB, the like-filtered AWGN noise contribution domi-

nates such that $P_G \gg N_b$ and (3.10) simplifies to,

$$SNR_A^{\text{dB}} \approx 10 \times log_{10}\left(\frac{S_t}{P_G}\right) \ . \tag{3.11}$$

Observation: The disparity between collected SNR_c and desired SNR_A results in $P_G \gg N_b$ and effectively simulates conditions for assessing performance under AWGN channel noise conditions.

3.3 Training and Classification

A total of N_B=1000 emissions per device were used for generating RF-DNA fingerprints and assessing classifier performance. The first 500 were used to generate "training" fingerprints $\mathbf{f}_\beta$ and the remaining 500 were used to generate "testing" fingerprints $\hat{\mathbf{f}}_\beta$, where subscript β denotes the type of fingerprint (TD, SD, GT, or GWT) used as described in Section 2.2. As in conventional classifier performance assessment, the set of $\mathbf{f}_\beta$ represents "known" data used for model development/classifier training and the set of $\hat{\mathbf{f}}_\beta$ represents previously "unseen" device emissions that were not used for model development/classifier training.

To improve model development robustness and analysis reliability, Monte Carlo training and classification were accomplished at each desired $SNR_A \in [-3.0, 27.0]$ dB using N_z=10 independent like-filtered AWGN noise realizations per device fingerprint and K=5-fold cross-validation. While the value of K can be data dependent, values of K=5 and K=10 are consistent with common practice [48]. K-fold cross-validation is a classifier model validation technique in which the training set of RF-DNA fingerprints is partitioned into K equally sized subsets. Classifier training is performed using $K-1$ subsets while the remaining subset is "held-out" for validation of the resulting model. The K-fold process is repeated a total of K times until each of the subsets have been "held out". Then the average correct classification performance is computed across all K trials. This process ensures that every RF-DNA fingerprint is "held out" exactly once and used for training $K-1$ times. Selection of the "best" *classification* model

was based on minimum *classification* error achieved across all noise realizations and cross-validation folds for each SNR_A.

3.3.1 MDA/ML Processing. The MDA/ML classifier was implemented as described in Section 2.3.1. Classifier model development was performed using N_B=500 $\mathbf{f}_\beta$ RF-DNA fingerprints and N_z=10 independent noise realizations per $\mathbf{f}_\beta$ at each investigated SNR. The "best" SNR-dependent model $\mathbf{W}_B$ was selected and a multivariate Gaussian fitted to projected $\mathbf{f}_\beta^{\mathbf{W}}$=$\mathbf{f}_\beta$×$\mathbf{W}_B$ fingerprints for each of the N_C classes using (2.24) and (2.25). *Classification* performance was then assessed using N_B=500 $\hat{\mathbf{f}}_\beta$ RF-DNA fingerprints and N_z=10 noise realizations per fingerprint at each investigated SNR_A; a total of 500×10=5000 independent Monte Carlo *classification* decisions per SNR_A.

For each test fingerprint $\hat{\mathbf{f}}_\beta$, the likelihood is computed for each of the N_C classes using the multivariate Gaussian models developed during training. The resultant *classification* decision for $\hat{\mathbf{f}}_\beta^{\mathbf{W}}$ being assigned to class c according to,

$$\underset{i}{\operatorname{argmax}} \left(P(c_i|\hat{\mathbf{f}}_\beta^{\mathbf{W}}) \right) \ , \tag{3.12}$$

where i=1, ..., N_C and $P(c_i|\hat{\mathbf{f}}_\beta^{\mathbf{W}})$ is the conditional posterior probability that $\hat{\mathbf{f}}_\beta^{\mathbf{W}}$ belongs to class c_i. Results for MDA/ML device *classification* performance are presented in Section 4.1 and Section 4.2 for RF-DNA fingerprints extracted from WiMAX and WiFi signals, respectively.

3.3.2 GRLVQI Processing. The GRLVQI classifier was implemented per Section 2.3.2 using the parameters in Table 3.2, where N_I is the number of iterations, N_f is the number of fingerprint features, and N_P is the number of prototype vectors. These specific parameter values were empirically selected based on a series of initial studies conducted using GT RF-DNA fingerprints, extracted from near-transient WiMAX transmissions at SNR_A=3.0 dB and N_C=3 devices, that resulted in consistent *classification* performance within reasonable computation times.

Table 3.2: GRLVQI Classifier Parameters.

	N_C	N_I	N_f	N_P
WiMAX	6	1200	204	10
WiFi	4	1200	363	10

As with MDA/ML processing, GRLVQI training and testing was accomplished using N_B=500 independent $\mathbf{f}_\beta$ and $\hat{\mathbf{f}}_\beta$ RF-DNA fingerprints and N_z=10 independent noise realizations per fingerprint at each investigated SNR. Accounting for the N_z=10 independent Monte Carlo noise realizations per fingerprint, all results presented in Chapter IV are based on 5000 independent *classification* decisions.

For each test fingerprint $\hat{\mathbf{f}}_\beta$, the GRLVQI *classification* process declares $\hat{\mathbf{f}}_\beta$ as belonging to class c according to,

$$\underset{c}{\operatorname{argmin}} \left(\sqrt{\sum_{i=1}^{N_f} \lambda_i \left(\hat{f}_i - p_i^{n,c} \right)^2} \right) , \tag{3.13}$$

where $\hat{f}_i$ is the i^{th} feature element of $\hat{\mathbf{f}}_\beta$, $\lambda_i \in \boldsymbol{\lambda}$ is the relevance ranking of the i^{th} feature, and $n=1, 2, \ldots, N_P$ with $\mathbf{p}^{n,c}$ being the n^{th} prototype vector associated with class model c. The resultant *classification* decision represents a one-to-many "best match" based on a Euclidean distance metric that has been used successfully in previous research [43, 64]. Results for GRLVQI device *classification* performance are presented in Section 4.1 and Section 4.2 for RF-DNA fingerprints extracted from WiMAX and WiFi signals, respectively.

3.4 Dimensional Reduction Analysis (DRA)

As noted in Section 2.3.2, one key advantage of the GRLVQI process over MDA/ML processing is that it inherently provides a measure ($\lambda_i \in \boldsymbol{\lambda}$ for $i=1, 2, \ldots, N_f$) for each RF-DNA fingerprint feature, the value of which indicates the relevance of that feature on the overall *classification* decision.

Process: Dimensional Reduction Analysis (DRA) is enabled by rank-ordering RF-DNA fingerprint features based on their relevance to overall *classification*. Once identified, a given number of less relevant features can be removed and lower dimensional fingerprints used for *classification* while maintaining a desired level of performance.

The "best" GRLVQI *classification* model $\mathbf{P}_B$ and associated relevance ranking $\boldsymbol{\lambda}^B$ are selected based upon the minimum *classification* error achieved across all noise realizations and cross-validation folds at each investigated SNR_A. Each $\boldsymbol{\lambda}^B$ is subsequently stored in a $N_S \times N_f$, where N_S is the number of SNR_A and N_f is the number of features comprising the RF-DNA fingerprints, matrix $\boldsymbol{\Lambda}^B$. Figure 3.2 shows representative "best" GRLVQI relevance values $\lambda_i^B \in \boldsymbol{\Lambda}_{h,i}^B$ for each SNR_A considered. Figure 3.2 clearly illustrates the dependence of feature relevance on SNR [72]. There are various strategies for selecting the "best" ranked dimensionally reduced feature sets based upon the relevance ranking values comprising $\boldsymbol{\Lambda}_{N_S \times N_F}^B$. Using a given relevance vector $\boldsymbol{\lambda}^B$ the indexes associated with the relevance values $\lambda_i^B \in \boldsymbol{\lambda}^B$ can be

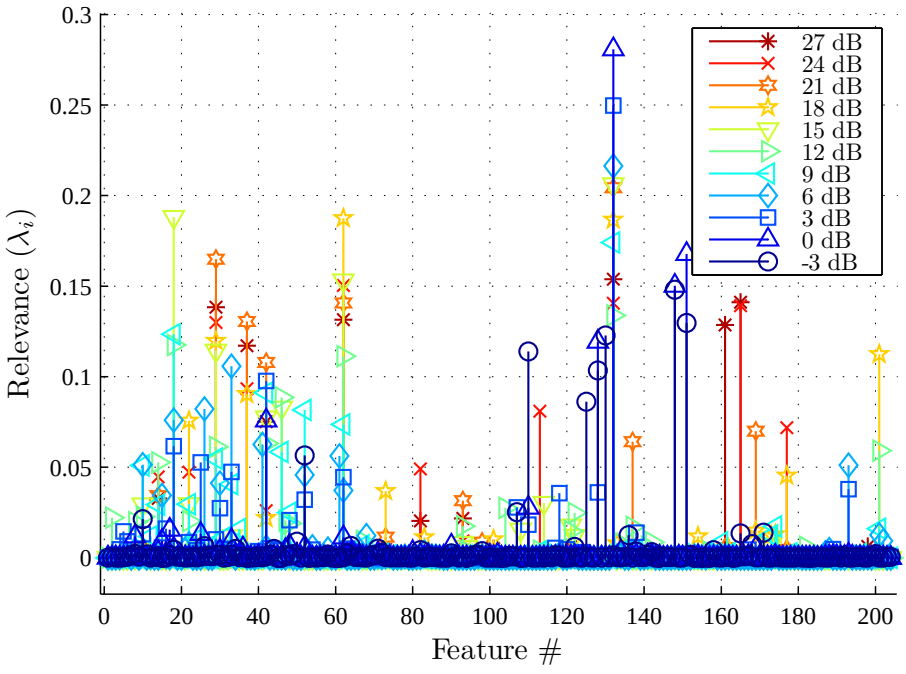


Figure 3.2: Overlay of WiMAX GT relevance rankings (λ_i^B) for a full-dimensional N_f=204 feature set at indicated SNR [72].

selected by,

$$f(\boldsymbol{\lambda}^B, \theta) = \left\{ i \in \mathsf{N} : \lambda_i^B \geq \theta \right\}, \tag{3.14}$$

$$f : \mathbb{R}^{N_f} \rightarrow \mathcal{P}(\mathsf{N}), \tag{3.15}$$

where θ is the relevance ranking selection threshold, i=$1, 2, \ldots, N_f$, N:=$\{1, 2, \ldots, N_f\}$, and $\mathcal{P}$ is the power set of N. This is extended to operate on the matrix $\boldsymbol{\Lambda}^B$ by,

$$f_h(\boldsymbol{\Lambda}^B, \Theta) = \left\{ i \in \mathsf{N} : \boldsymbol{\Lambda}_{h,i}^B \geq \theta_h \right\} \tag{3.16}$$

where $\Theta = (\theta_1, \ldots, \theta_{N_S})$ and h=$1, 2, \ldots, N_S$. This work considers four methods for selecting DRA subsets, based upon $\boldsymbol{\Lambda}^B$, for the DRA results presented in Section 4.1.3 and Section 4.2.3. Using (3.16), the four DRA methods are implemented as [72]:

1. ***DRA Method #1***: Uses highest ranked relevance values generated at a single SNR to assess *classification* performance at all SNR and selected according to,

$$\boldsymbol{\lambda}_j^R \in f_j(\boldsymbol{\Lambda}_{j,\star}^B, \theta_j), j \in h, \tag{3.17}$$

   where h=$1, 2, \ldots, N_S$, $\boldsymbol{\lambda}_j^R$ is a vector of the relevance values selected from the j^{th} row of matrix $\boldsymbol{\Lambda}^B$ according to (3.14) .

2. ***DRA Method #2***: Uses highest ranked relevance values for each SNR considered to assess *classification* performance at that same SNR and chosen by,

$$\boldsymbol{\lambda}_h^R \in f_h(\boldsymbol{\lambda}_{h,\star}^B,\ \theta_h), \tag{3.18}$$

   where h=$1, 2, \ldots, N_S$ and $\boldsymbol{\lambda}_h^R$ is a vector comprised of the relevance values that satisfy (3.16) at the selected SNR.

3. ***DRA Method #3***: Uses highest ranked relevance values based on the average relevance rankings calculated across all SNR considered and selected by,

$$\overline{\boldsymbol{\lambda}}^{R} \in f\left(\frac{1}{N_S}\sum_{i=1}^{N_f}\boldsymbol{\Lambda}^{B}_{\star,i}\,,\theta\right), \tag{3.19}$$

where $\overline{\boldsymbol{\lambda}}^{R}$ is the reduced average feature relevance rankings selected by (3.14).

4. ***DRA Method #4***: Uses the union of the highest ranked relevance values across all SNR considered and chosen according to,

$$\breve{\boldsymbol{\lambda}}^{R} \in \bigcup_{h=1}^{N_S} f_h\left(\boldsymbol{\Lambda}^{B},\Theta\right). \tag{3.20}$$

where $\breve{\boldsymbol{\lambda}}^{R}$ is a vector of relevance ranking values that are the union of all $\lambda^{B}_{h,i}\in\boldsymbol{\Lambda}^{B}$ that satisfy (3.16).

Figure 3.3 provides an illustration of the highest ranked relevance ranking values for each of the four methods and selected according to (3.16).

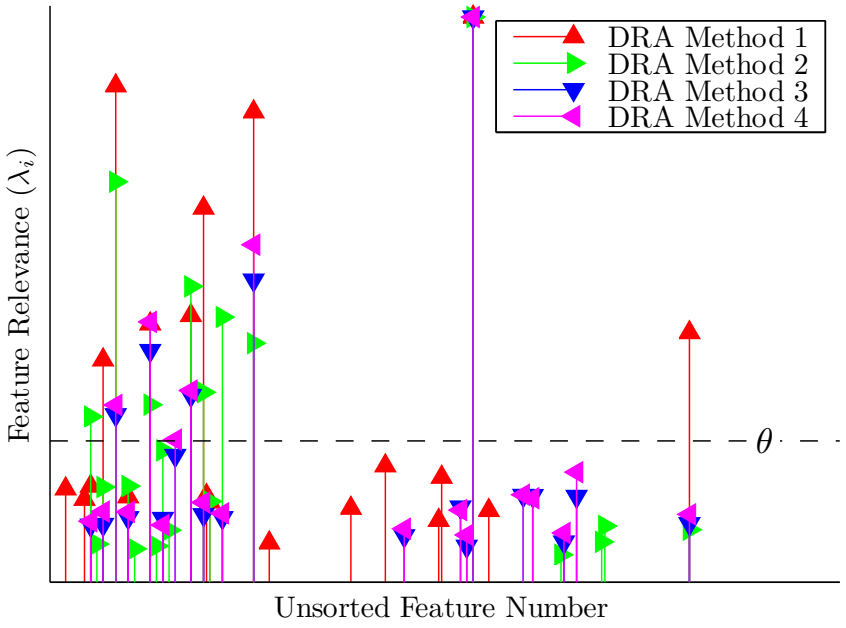


Figure 3.3: Overlay of highest relevance ranking values using each of the four DRA methods and the selection operation in (3.16).

3.5 Device Bit-Level ID Verification

As outlined in Section 2.4, the one-to-one bit-level ID *verification* process for devices differs from the one-to-many "best match" *classification* process. Specifically, the ID *verification* process generates a measure of similarity that indicates "how much" an *unknown* device's current RF-DNA fingerprint matches the stored true reference model associated with the *claimed* identity being presented by the *unknown* device [20, 71–73]. The *unknown* device is either authorized or rogue and presents bit-level credentials (e.g., MAC address, IMEI number, SIM number, etc.) to the network for authentication. The one-to-one ID *verification* process is used here to assess two scenarios:

1. *Authorized Device ID* Verification: Granting network access to authorized users presenting **proper** bit-level credentials.
2. *Rogue Device Detection*: Denying network access to unauthorized rogue devices presenting **false** bit-level credentials.

The device *verification* process is implemented using a measure of similarity, or *verification* test statistic z_v, that can be based on 1) statistical measures such Bayesian posterior probability as in [20, 29, 71], 2) geometric measures such as Euclidean distance, spatial angle, etc. [72, 73], or 3) some combination thereof.

3.5.1 MDA/ML Processing. For MDA/ML device ID *verification*, the similarity measure z_v is generated from normalized a posterior probability. This is done using a collection of input testing fingerprints $\hat{\mathbf{f}}_\beta$ from an "unknown" device (authorized or rogue) and projection matrix $\mathbf{W}_B$ from MDA/ML training using N_C^A authorized devices. The projected "unknown" fingerprint responses are calculated as $\hat{\mathbf{f}}_\beta^{\mathbf{W}}=\hat{\mathbf{f}}_\beta\times\mathbf{W}$ and used to calculate N_C^A conditional probabilities representing a measure of "how much" $\hat{\mathbf{f}}_\beta^{\mathbf{W}}$ looks like each of the "authorized" device models. The resultant posterior probability vector for each input $\hat{\mathbf{f}}_\beta^{\mathbf{W}}$ is given by,

$$\mathbb{P} = \left[P(c_1|\hat{\mathbf{f}}_\beta^{\mathbf{W}}), P(c_2|\hat{\mathbf{f}}_\beta^{\mathbf{W}}), \ldots, P(c_{N_C^A}|\hat{\mathbf{f}}_\beta^{\mathbf{W}})\right] \ , \tag{3.21}$$

and subsequently normalized as,

$$\bar{\mathbb{P}} = \frac{\mathbb{P}}{\sum_{i=1}^{N_C} \mathbb{P}_i} \ . \tag{3.22}$$

For ID *verification*, the resultant decision is binary and the device's claimed identity is deemed authentic (rightly or wrongly) when the normalized a posterior probability $\bar{\mathbb{P}}$ in (3.22) meets or exceeds a predetermined threshold:

$$z_v^{\bar{\mathbb{P}}} = \bar{P}(c|\hat{\mathbf{f}}_\beta^{\mathbf{W}}) \geq t_v, \tag{3.23}$$

where c is the class the device has claimed to belong, and t_v is the *verification* decision threshold. If the posterior probability fails to meet the *verification* decision threshold, the device is deemed to be an impostor/impersonator (rightly or wrongly) and denied network access.

The impact of varying threshold t_v in (3.23) is illustrated using the representative In-Class and Out-of-Class Probability Mass Functions (PMF) in Fig. 3.4 for an arbitrary test statistic z_v. The In-Class PMF is generated using z_v for the case when an *unknown* device presents *proper* bit-level credentials matching an authorized device and the *unknown* device is, in fact, the authorized device. The corresponding in-class probability is denoted by,

$$p(z_v|C_i\,, D_i)\ , \tag{3.24}$$

where C_i is the ID "claimed" by the *unknown* device and D_i is the "actual" *unknown* device's ID. The Out-of-Class PMF is generated using z_v for the case when an *unknown* device *falsely* presents bit-level credentials of an authorized device but is in fact a "rogue" device posing as an authorized device. The corresponding out-of-class probability is denoted by,

$$p(z_v|C_i\,, D_j), \tag{3.25}$$

where $j = 1, 2, \ldots, N_C$ and $i \neq j$.

Varying the value of t_v over the interval of $[0, 1]$ in Fig. 3.4 yields varying levels of network security which correlate to achieving either 1) reduced rogue device access error (i.e., reducing the out-of-class shaded area right of t_v) or 2) reduced authorized device rejection error (i.e., reducing the in-class unshaded area left of t_v) [24, 53]; the inability to simultaneous achieve both of these desired effects is evident for the given PMFs shown in Fig. 3.4.

3.5.2 GRLVQI Processing. As done for GRLVQI *classification* in Section 3.3.2, composite *testing* fingerprints $\hat{\mathbf{f}}_\beta$ for an *unknown* device are used for device ID *verification*. Given the p^{th} GRLVQI prototype vector from class c ($\mathbf{p}^{n,c}$), four similarity measures were considered for GRLVQI processing, including:

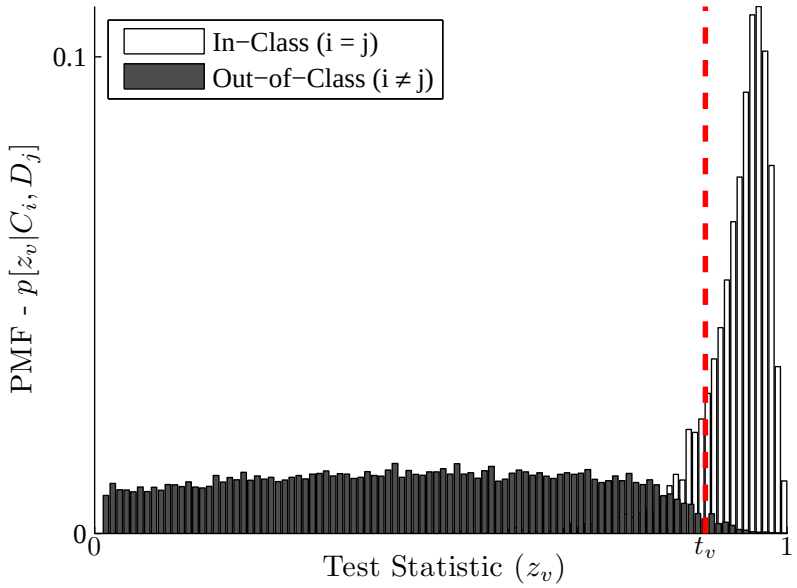


Figure 3.4: Representative In-Class (unfilled) and Out-of-Class (filled) Probability Mass Functions (PMFs) for arbitrary test statistic z_v using a *traditional* verification threshold t_v in (3.23).

1. A *Weighted Euclidean Distance* metric calculated as,

$$z_v^d(n,c) = \sqrt{\sum_{i=1}^{N_f} \lambda_i \left(\hat{f}_i - p_i^{n,c}\right)^2}\ , \tag{3.26}$$

   where $\hat{f}_i \in \hat{\mathbf{f}}_\beta$ and $p_i^{n,c} \in \mathbf{p}^{n,c}$.

2. A *Normalized Euclidean Distance* metric calculated as,

$$z_v^{\bar{d}}(n,c) = \frac{z_v^d(n,c)}{\sqrt{\sum_{i=1}^{N_f}\left(\hat{f}_i\right)^2}\cdot\sqrt{\sum_{i=1}^{N_f}\left(p_i^{n,c}\right)^2}}\ . \tag{3.27}$$

3. A *Spatial Angle* metric calculated as,

$$z_v^{\theta}(n,c) = cos^{-1}\left[Z^{\theta}(n,c)\right]\ , \tag{3.28}$$

where,

$$Z^{\theta}(n,c) = \frac{\sum_{i=1}^{N_f} \hat{f}_i p_i^{n,c}}{\sqrt{\sum_{i=1}^{N_f} \left(\hat{f}_i\right)^2} \cdot \sqrt{\sum_{i=1}^{N_f} \left(p_i^{n,c}\right)^2}} \ .$$

4. A *Distance-Angle Product* metric calculated directly from (3.27) and (3.28) as,

$$z_v^{\bar{d}\theta}(n,c) = z_v^{\bar{d}}(n,c) \times z_v^{\theta}(n,c) \ . \tag{3.29}$$

Motivation: Introduction of the *Distance-Angle Product* metric was motivated by the fact that the GRLVQI classifier assigns an unknown fingerprint to a given class based upon minimum distance. The idea is to bias the process to select prototype vectors having both small spatial angle and minimum distance to the unknown fingerprint.

The test statistic mean (μ_z) and standard deviation (σ_z) are calculated for a given z_v from (3.26) through (3.29) and corresponding PMFs for each of the N_C^A classes used for device ID *verification*. A device's claimed identity is correctly or incorrectly verified according to a binary decision based upon,

$$-t_v \leq z_v \leq t_v \ , \tag{3.30}$$

where t_v is the *verification* threshold given by

$$t_v = \mu_z + (\eta \cdot \sigma_z) \ , \tag{3.31}$$

with η controlling the span of a window centered about class mean μ_z. The *unknown* device is declared rogue (rightly or wrongly) if z_v falls outside the *verification* window.

This GRLVQI *verification* thresholding process is illustrated using the representative In-Class (unfilled bars) and Out-of-Class (filled bars) *verification* PMFs in Fig. 3.5 for an arbitrary z_v, with the PMFs generated per (3.24) and (3.25), respectively. As with MDA/ML-based *verification*, the In-Class PMF reflects a measure of "how much" current fingerprints from authorized device c match the stored reference model associated with the actual/true bit-level credentials for device c. The Out-of-

Class PMF reflects a measure of "how much" current fingerprints from an *unknown* device, either an authorized or previously "unseen" rogue device falsely presenting "claimed" bit-level credentials for device c that differ from its own, matches the stored reference model associated with the "claimed" bit-level credentials for device c.

GRLVQI device ID *verification* performance in Chapter IV is evaluated using PMFs similar to those in Fig. 3.5 by varying threshold $t_v(\eta)$ and generating conventional *verification* outcomes (rates) as shown in Table 2.1 [20,24,53] and reintroduced here as Table 3.3 for completeness. If the "unknown" device is an authorized device presenting correct bit-level credentials, True Verification Rate (TVR) provides a direct measure of the *Authorized Device Verification Rate* (ADVR). If the "unknown" device is a rogue device presenting false bit-level credentials, the TVR outcome corresponds to falsely granting network access and the *Rogue Device Detection Rate* (RDDR) can be calculated as RDDR=1−TVR.

Typical rate behavior is illustrated in Fig. 3.6 for variation in $t_v(\eta)$. Rate tradeoffs are quantitatively assessed using a Receiver Operating Characteristic (ROC) curve

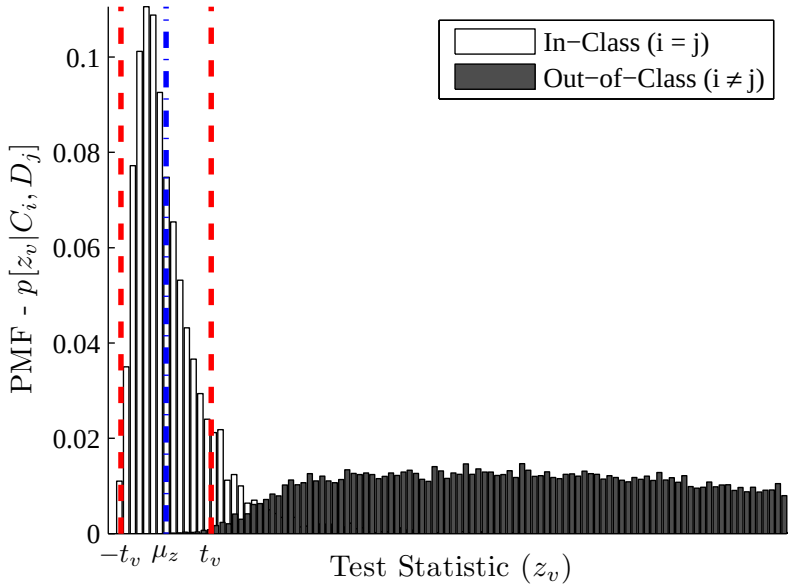


Figure 3.5: Representative In-Class (unfilled) and Out-of-Class (filled) Probability Mass Functions (PMFs) for arbitrary test statistic z_v using a *modified* verification threshold t_v in (3.30) [72].

Table 3.3: Verification Outcomes & Rates.

	System Declaration (Rate)	
Actual	Authorized	Rogue
Authorized	True Verification (TVR)	False Reject (FRR)
Rogue	False Verification (FVR)	True Reject (TRR)

and associated Equal Error Rate (EER) point as shown in Fig. 3.7 [34]. To characterize ADVR for authorized devices, ROC results in Chapter IV are generated as TVR versus False Verification Rate (FVR). For rogue RDDR characterization, ROC results generated as TVR versus Rogue Accept Rate (RAR).

Presentation: ROC EER points are presented in figures for reference only and to enable qualitative visual assessment. They are not intended to represent optimal operating points for either the proof-of-concept results presented herein or envisioned operational applications.

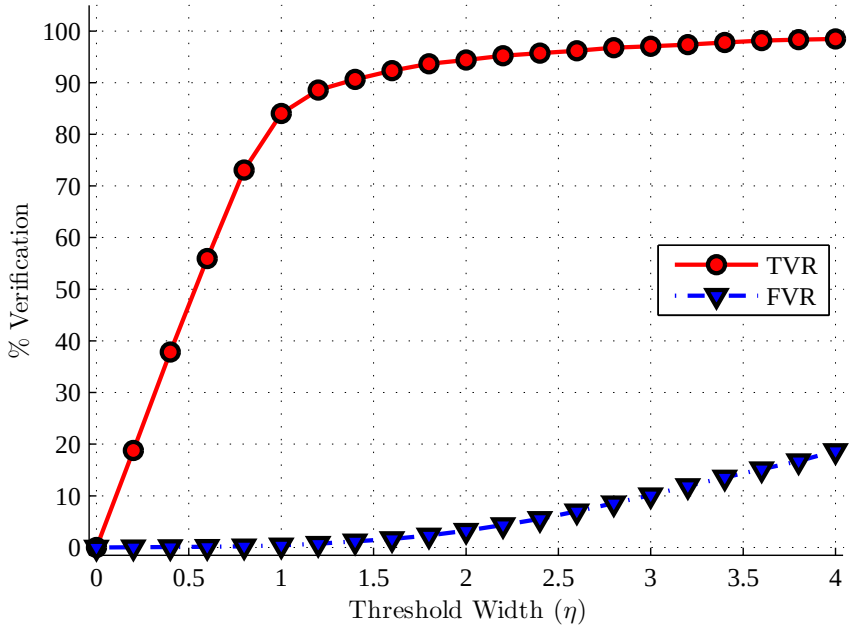


Figure 3.6: Percent correct (True) and incorrect (False) ID *verification* versus threshold width (η) [72].

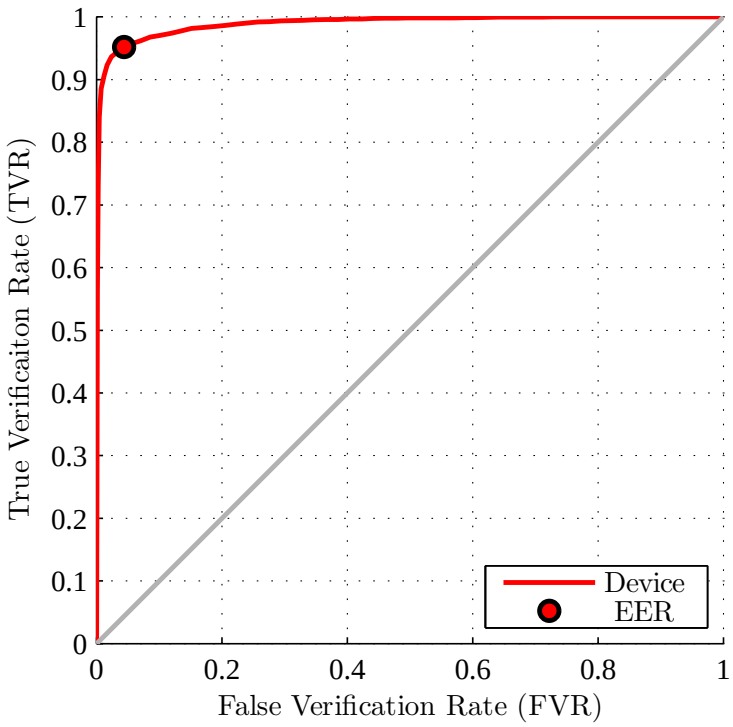


Figure 3.7: ROC curve for True Verification Rate (TVR) vs. False Verification Rate (FVR) and corresponding EER point [72].

IV. Device Classification and ID Verification Results

This chapter presents results and analysis for *classification* and *verification* of IEEE 802.16e WiMAX and 802.11a WiFi devices using the the Multiple Discriminant Analysis, Maximum Likelihood (MDA/ML) and Generalized Relevance Learning Vector Quantized-Improved (GRLVQI) classifiers described in Section 2.3.1 and Section 2.3.2, respectively. Section 4.1 presents results for 802.16e WiMAX devices and Section 4.2 presents results for 802.11a WiFi devices. This includes *classification* results using 1) a full-dimensional feature set in Section 4.1.1 and Section 4.1.2 for WiMAX and Section 4.2.1 and Section 4.2.2 for WiFi, and 2) reduced dimensional feature sets in Section 4.1.3 (WiMAX) and Section 4.2.3 (WiFi). Section 4.1.4 and Section 4.2.4 present *verification* performance results for both authorized and rogue devices operating within a WiMAX and WiFi network, respectively.

The RF-DNA fingerprints used for demonstration were based on 1D Time Domain (TD), 1D Spectral Domain (SD), 2D Gabor Transform (GT), and 2D Gabor-Wigner Transform (GWT) features as indicated. The RF-DNA features were generated from N_B=1000 signal responses per device in accordance with the methodologies detailed in Section 2.2.1 (TD), Section 2.2.2 (SD), and Section 2.2.3 (GT and GWT). The resultant TD, SD, GT, or GWT fingerprints were comprised of N_f total RF-DNA features with the value of N_f depending on fingerprint type and assessment objectives. For 802.16e WiMAX results in Section 4.1 and 802.11a WiFi results in Section 4.2, the MDA/ML classifier was implemented using procedures described in Section 2.3.1 and Section 3.3.1 and the GRLVQI classifier was implemented using procedures described in Section 2.3.2 and Section 3.3.2.

To facilitate direct comparison of MDA/ML and GRLVQI fingerprinting techniques, the same set of RF-DNA fingerprints ($\mathbf{F}_{1000\times N_f}$), with each fingerprint generated using an independent Additive White Gaussian Noise (AWGN) realization, was input to both classifiers. This enabled reliable comparative assessment based on 95% Confidence Intervals (CI=95%) using Monte Carlo simulation.

Presentation: To enhance visual clarity and qualitative assessment, the CI=95% intervals are intentionally omitted from all figures. However, all figure data markers (squares, circles, triangles, etc.) have been appropriately sized such that their vertical extent exceeds the CI=95% interval. Thus, overlapping data markers which encompass data mean values represent statistically identical results while non-overlapping data markers represent statistically different results.

Consistent with common best practices used in pattern recognition [48], the selected collection of N_B=1000 RF-DNA fingerprints (TD, SD, GT, or GWT) was partitioned into two subsets:

1. The first subset of $\mathbf{F}$ was used for classifier *training* and *validation* of the developed device reference model. The "best" reference model ($\mathbf{W}_B$ for MDA/ML and $\mathbf{P}_B$ for GRLVQI) was selected by tracking *classification* during K-fold cross-validation and selecting the fold model that yielded minimum *classification* error (1-%C) across all K=5 cross-validation folds and N_z=10 AWGN realizations.
2. The second subset of $\mathbf{F}$ was used for "blind" *testing* the classifier to assess the "best" model's ($\mathbf{W}_B$ or $\mathbf{P}_B$) *classification* performance using previously unseen RF-DNA fingerprints, i.e., fingerprints not used for classifier training or validation in Step 1. All results presented herein are based on classifier performance using the "blind" test set of RF-DNA fingerprints.

The procedures in Section 3.1 and Section 3.2 were applied to generate RF-DNA fingerprint sets at the desired SNR. This includes extraction of N_B=1000 complex bursts from collected signal records, down-conversion and digital baseband filtering, and the addition of power-scaled AWGN realizations to achieve the desired *Analysis* SNR_A.

Presentation: While notationally introduced as SNR_A for development in Chapter III, the subscript A is henceforth dropped and SNR simply used throughout the remainder of this chapter.

4.1 IEEE 802.16e WiMAX Results

WiMAX Device *classification* and *verification* results were generated using selected RF-DNA fingerprints extracted from emissions of six like-model 802.16e WiMAX MS devices–denoted herein as ID #s MS63A7, MS63A9, MS66E7, MS6373, MS6387, MSD905; thus, serial number discrimination was assessed. The procedures in Section 3.1 and Section 3.2 were applied to generate RF-DNA fingerprint sets having a total of N_B=1000 complex bursts per device. In accordance with Section 3.2, the collected signals were digitally filtered, individual bursts detected and removed from the overall collection record, and the SNR scaled to achieve the desired *Analysis* SNR_A.

Assessment results in this chapter are for $SNR \in [-3.0, 27.0]$ dB in 3.0 dB increments, with the SNR scaling process was repeated N_z=10 times to ensure sufficient statistical significance for Monte Carlo analysis. For WiMAX assessment, the full-dimensional TD, SD, GT, or GWT fingerprints were comprised of N_f=[72, 24, 204, 204]. Results are first presented for full-dimensional RF-DNA fingerprinting in Section 4.1.1 and Section 4.1.2 followed by reduced dimensional fingerprinting results in Section 4.1.3.

4.1.1 Full-Dimensional WiMAX Classification: MDA/ML. Figure 4.1 shows cross-device average and individual device MDA/ML Correct Classification Percentage (%C) using TD, SD, GT, and GWT RF-DNA fingerprints for $SNR \in [-3.0, 27.0]$ dB. Figure 4.1(a) shows MDA/ML performance using TD RF-DNA fingerprints (N_f=72 features) and reflects 1) cross-device average *classification* performance of %C≥90% for $SNR \geq$15.0 dB, and 2) individual device %C≥90% for 5 of 6 WiMAX MS devices. As indicated in Fig. 4.1(b), performance with SD RF-DNA features is considerably poorer with %C≥90% achieved for only one device (MSD905) at $SNR \geq$12.0 dB. Figure 4.1(c) and Fig. 4.1(d) present performance using joint T-F domain fingerprints generated using GT and GWT features, respectively. From a cross-device average perspective, GT features are superior with %C≥90% achieved for $SNR \geq$7.5 dB. This represents a "gain" of $G_p \approx$4.5 dB relative to GWT RF-DNA fingerprinting which requires $SNR \geq$12.0 dB to achieve average performance of %C≥90%.

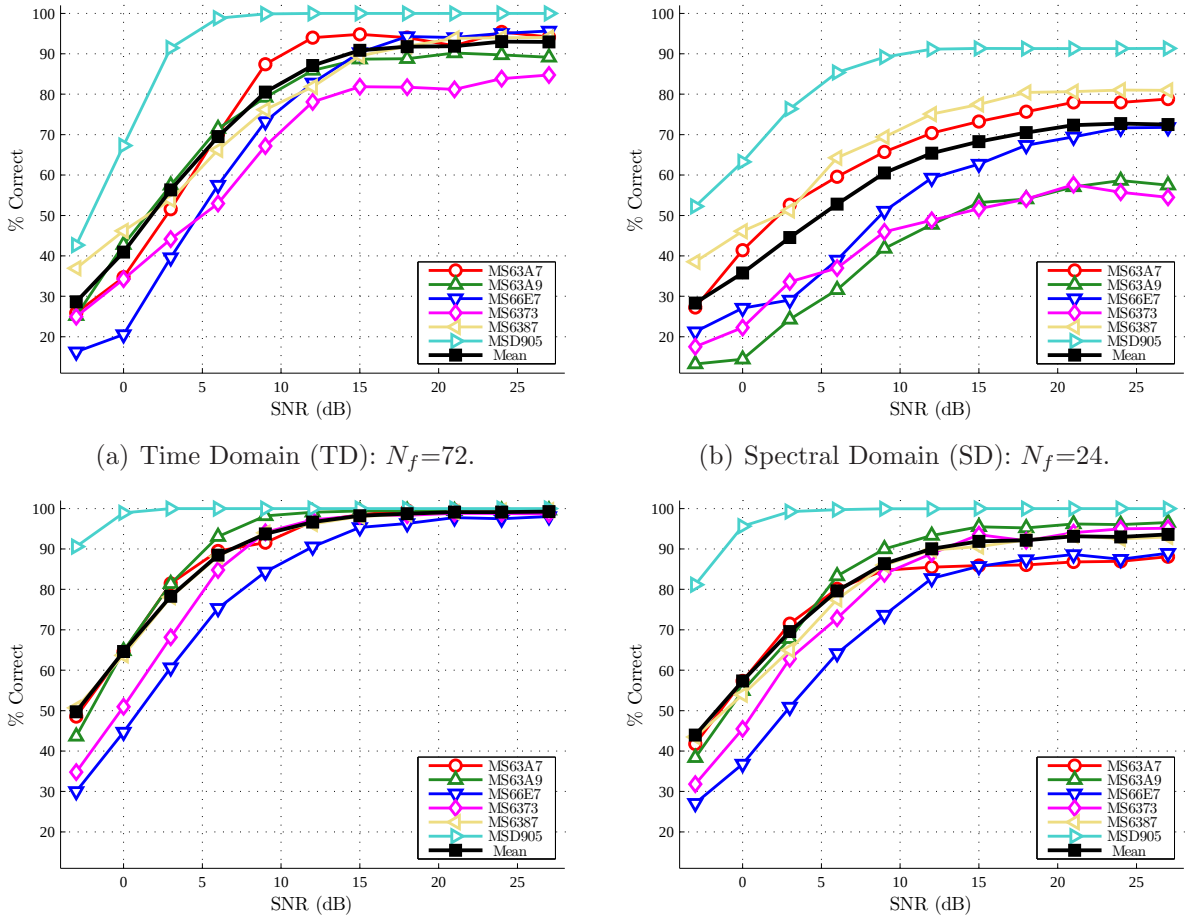
Definition: Gain (G_p): Reduction in required SNR, in dB, for two methods to achieve a given %C *classification* performance.

The superiority of GT features is also evident when analyzing individual device performances. GT feature results in Fig. 4.1(c) show that all devices achieve the %C≥90% benchmark for SNR≥12.0 dB. This is in sharp contrast to GWT results in Fig. 4.1(d) which show that two devices (MS63A7 and MS66E7) never reach the %C≥90% benchmark for all SNR considered. Based upon results in Fig. 4.1, it is concluded that GT RF-DNA features are the best alternative for achieving serial number *classification* of 802.16e WiMAX MS devices when using MDA/ML processing.

General: The underlying factors for GT feature superiority, relative to what is achieved with GWT features, was not of primary interest. Recall that GWT features were introduced as a means to assess linear versus non-linear feature performance in a multipath environment.

Note: The superiority of GT fingerprinting in Fig. 4.1 is not attributable to the larger number of full-dimensional features being used. This is subsequently demonstrated using DRA in Section 4.1.3.

4.1.2 Full-Dimensional WiMAX Classification: GRLVQI. Full-dimensional GRLVQI *classification* performance was assessed using the same six WiMAX MS devices used for *classification* assessment in Section 4.1.1. Individual device as well as average GRLVQI %C performance using TD, SD, GT, and GWT RF-DNA fingerprints at $SNR\in[-3.0, 27.0]$ dB is shown in Fig. 4.2. For TD RF-DNA fingerprints, two of six individual WiMAX MS devices (MS634A7 and MSD905) achieve 90% or better correct *classification* at SNR≥9.0 dB. *Classification* of MS6387 is individually classified correctly at 90% for 15≤SNR≥21.0 dB; however, individual *classification* of the remaining WiMAX devices fails to achieve %C=90% using TD RF-DNA fingerprints, Fig. 4.2(a). Average GRLVQI *classification* using TD fingerprints is 90% or better for SNR≥24.0 dB. Figure 4.2(b) illustrates individual device and average



(a) Time Domain (TD): N_f=72.

(b) Spectral Domain (SD): N_f=24.

(c) Gabor Transform (GT): N_f=204

(d) Gabor-Wigner Transform (GWT): N_f=204

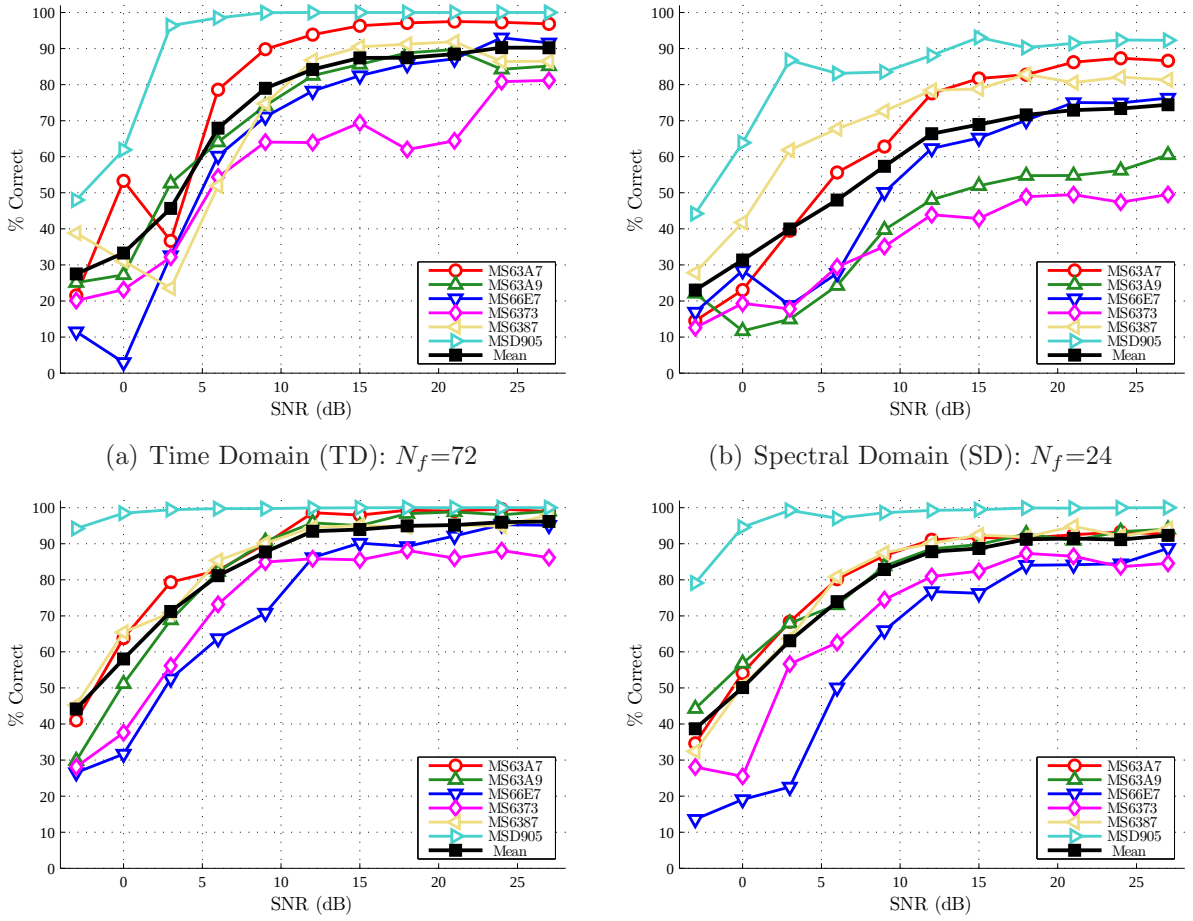
Figure 4.1: Full-Dimensional MDA/ML *classification* performance using TD, SD, GT and GWT RF-DNA features from six 802.16e WiMAX devices [76].

classification performance using SD RF-DNA fingerprints. The GRLVQI classifier correctly identifies device MSD905 with %C=90% certainty for $SNR \geq 15.0$ dB. All other individual devices as well as average *classification* performance fails to achieve the %C=90% benchmark. Figure 4.2(c) provides an illustration of individual as well as average device GRLVQI *classification* performance using GT–based RF-DNA fingerprints. Individual device *classification* performance is 90% or better for all WiMAX MS devices, except MS6373, for $SNR \geq 15.0$ dB. MSD905 is corretly classified at 90% or better for all investigated SNRs. Average device *classification* performance is 90% or better for $SNR \geq 12.0$ dB.

GRLVQI individual and average device *classification* performance, using GWT RF-DNA fingerprints, is shown in Fig. 4.2(d). As with GT fingerprint *classification* performance, MSD905 is correctly identified at a rate of 90% or better for $SNR \in [-3.0, 27.0]$ dB. In comparison to GT–based *classification* results, individual *classification* of MS66E7 using GWT RF-DNA fingerprints never achieves the %C=90% benchmark; representing a performance degradation. The average device *classification* performance suffers a 3.0 dB loss, dropping from SNR=12.0 to 15.0 dB, when switching from GT to GWT RF-DNA fingerprints. Results in Fig. 4.2 illustrate that GRLVQI *classification* using GT RF-DNA fingerprints provides the best means for achieving serial number *classification* of 802.16e WiMAX MS devices.

Note: The superiority of GT fingerprinting in Fig. 4.2 is not attributable to the larger number of full-dimensional features being used. This is subsequently demonstrated using DRA in Section 4.1.3.

Figure 4.3 provides a direct comparison between average device *classification* performance of the MDA/ML and GRLVQI classifiers. Clearly MDA/ML results in the best average *classification* performance; however, GRLVQI classifier performance is within 10% of the MDA/ML results. Although GRLVQI does not achieve the same degree of individual and average device *classification* performance, as that of MDA/ML, it addresses one key shortfall of the MDA/ML classifier in that GRLVQI provides a direct measure of how much each individual feature, that comprise an



(a) Time Domain (TD): N_f=72

(b) Spectral Domain (SD): N_f=24

(c) Gabor Transform (GT): N_f=204 [72]

(d) Gabor-Wigner Transform (GWT): N_f=204)

Figure 4.2: Full-Dimensional GRLVQI *classification* performance using TD, SD, GT and GWT RF-DNA features from six 802.16e WiMAX devices.

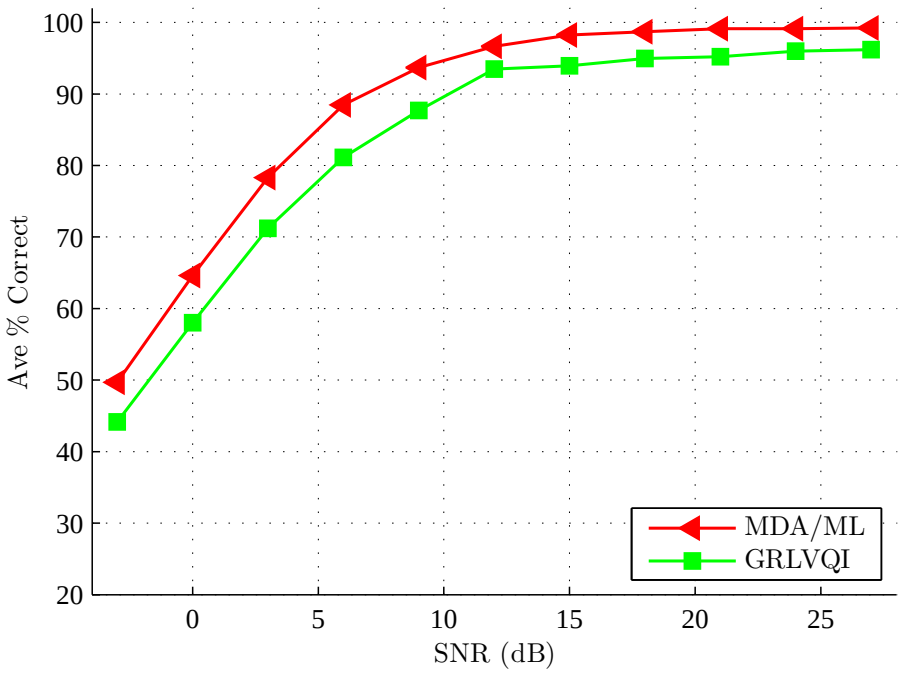


Figure 4.3: Cross-device average MDA/ML and GRLVQI *classification* performance for 802.16e WiMAX devices using Gabor Transform (GT) RF-DNA features.

RF-DNA fingerprint, contributes to a *classification* decision. This measure of feature contribution is defined as its relevance ranking, as defined in Section 2.3.2, and enables Dimensionality Reduction Analysis (DRA).

4.1.3 DRA Impact on WiMAX Classification. This section provides Dimensionality Reduction Analysis (DRA) results using the four strategies for selection of the "best" ranked dimensionally reduced feature sets as described in Section 3.4. Prior to generation of MDA/ML and GRLVQI *classification* performance for $SNR \in [-3.0, 27.0]$ dB, an initial assessment was performed using relevance values selected using (3.17) for SNR=12.0 dB (j=6) to assess DRA impact on *classification* performance. Initial DRA impact on device *classification* was assessed using three reduced subsets selected using the relevance values $\boldsymbol{\lambda}_6^R \in f_6(\boldsymbol{\Lambda}_{6,\star}^B, \theta_6)$ and comprised of the:

1. Highest ranked 10% features (DRA_1=90%).

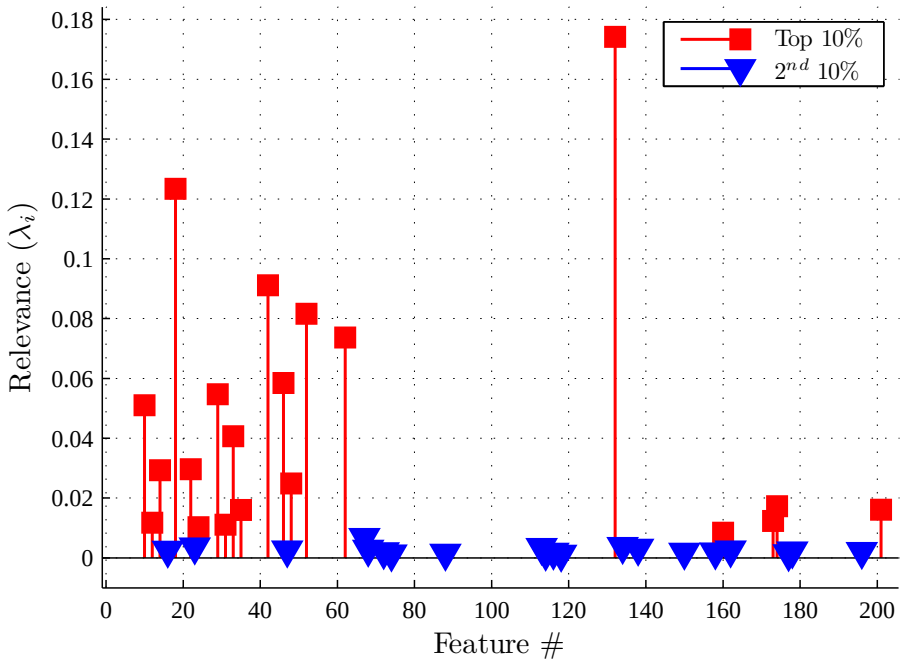


Figure 4.4: GRLVQI λ_i relevance values for highest ranked 10% (squares) and second-highest ranked 10% (triangles) at SNR=12.0 dB [72].

2. Second highest ranked 10% features (DRA_2=90%).

3. Highest ranked 20% features–union of DRA_1 and DRA_2 (DRA_3=80%).

Corresponding λ_i values for the two 10% subsets extracted from Fig. 3.2 are shown in Fig. 4.4. It is clear that the λ_i values for the second-highest ranked 10% are much lower than the highest ranked 10%; thus indicating that these features contribute very little to the *classification* decision.

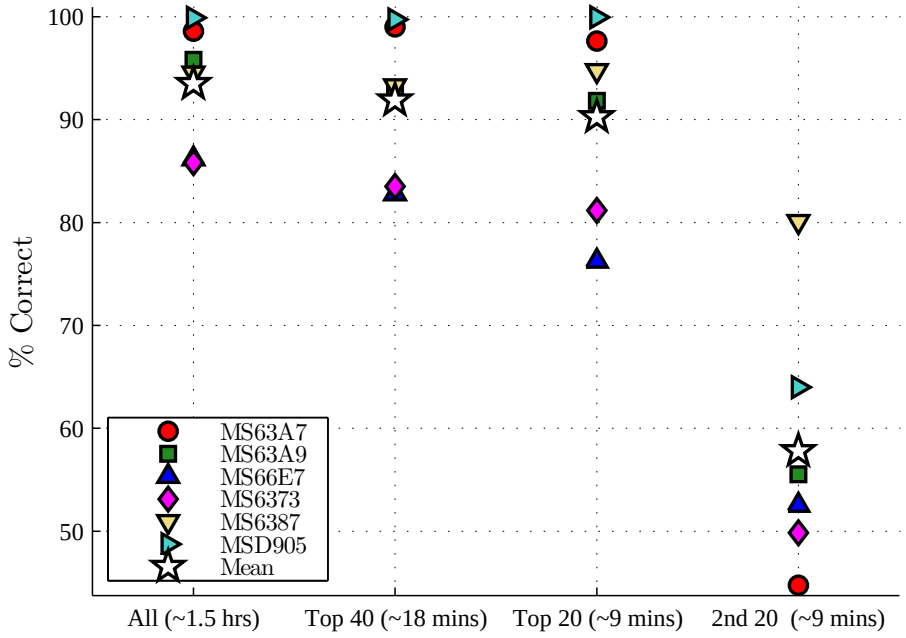
Based upon the full-dimensional *classification* results presented in Section 4.1.1 and Section 4.1.2, GT-based RF-DNA fingerprints extracted from WiMAX near-transient responses are used to assess the effectiveness of the GRLVQI classifier's assigned feature rankings $\mathbf{\Lambda}^B$. The effectiveness of the GRLVQI feature ranking process is illustrated in Fig. 4.5(a) which shows GRLVQI device *classification* performance for the reduced-feature subsets described above, as well as performance using all N_f=204 features. Approximate computation times are shown along the horizontal

axis in parenthesis for each case. Based upon these results it is clearly evident that the GRLVQI process is *very effective* in ranking relevant *classification* features. This conclusion is reinforced by several observations:

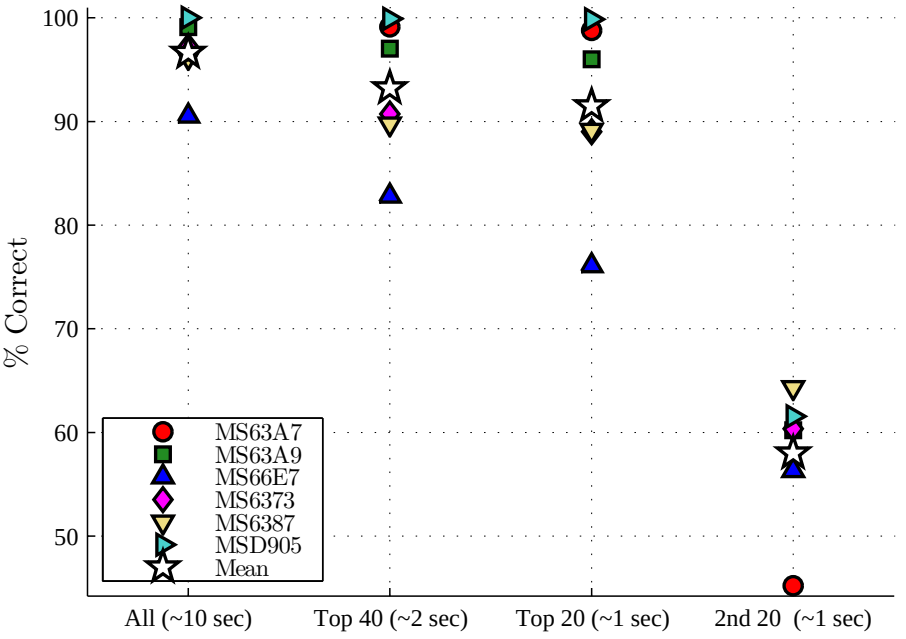
1. Performance with the 20 highest ranked (top 10%) features is statistically equivalent to full-dimensional performance and yields a significant 10× reduction in required computation time.
2. Performance with the second-highest 20 ranked features is considerably poorer than that of full-dimensional performance, with device *classification* degrading by 5% to 30%.
3. Performance using the highest 40 ranked features is statistically equivalent to performance using the highest 20 ranked features. This suggests that the additional 20 features are either irrelevant or contain redundant information and a 2× processing penalty is incurred.

As a final independent assessment of GRLVQI DRA effectiveness, the identical reduced feature sets were used with the MDA/ML classifier described in Section 2.3.1. Reduced dimension MDA/ML *classification* results are presented in Fig. 4.5(b) along with full-dimensional results for comparison. With regard to *classification* performance, MDA/ML results and conclusions are consistent with GRLVQI results in Fig. 4.5(a). However, MDA/ML results using the highest ranked 10% features only required approximately $1/300^{th}$ of the GRLVQI computation time. The added "insight" that GRLVQI provides is clearly beneficial, but it does come at a cost.

The patches providing greatest discriminating information are highlighted in Fig. 4.6. This figure shows the T-F responses for arbitrary bursts from each of the six authorized devices (MS63A7, MS63A9, MS66E7, MS6373, MS6387, MSD905). The red rectangles identify patch locations containing the highest ranked 10% features as shown in Fig. 4.4 and used to generate results in Fig. 4.5. As indicated, discrimination is not solely obtained from information contained in T-F patches containing higher level signal responses.



(a) GRLVQI Processing



(b) MDA/ML Processing

Figure 4.5: WiMAX Dimensional Reduction Analysis (DRA): Full-dimensional (All) vs. three DRA feature sets comprised of highest ranked 10% (Top 20), highest ranked 20% (Top 40), and second-highest ranked 10% (2nd 20) features at SNR=12.0 dB [72].

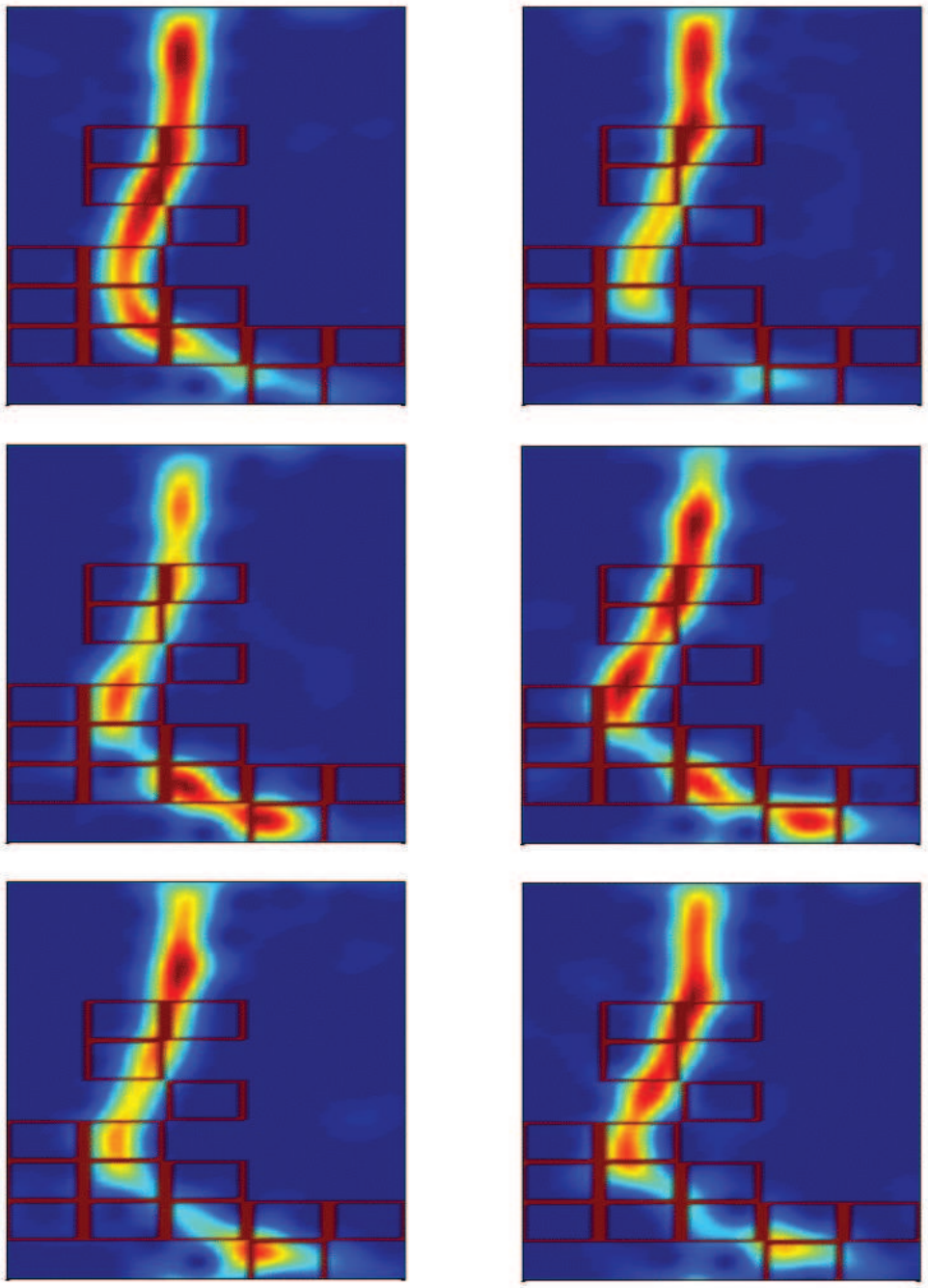


Figure 4.6: Gabor T-F responses for N_C=6 WiMAX devices: Rectangular patches identify regions containing the highest ranked 10% (Top 20) features in Fig. 4.4. One representative response shown per device [72].

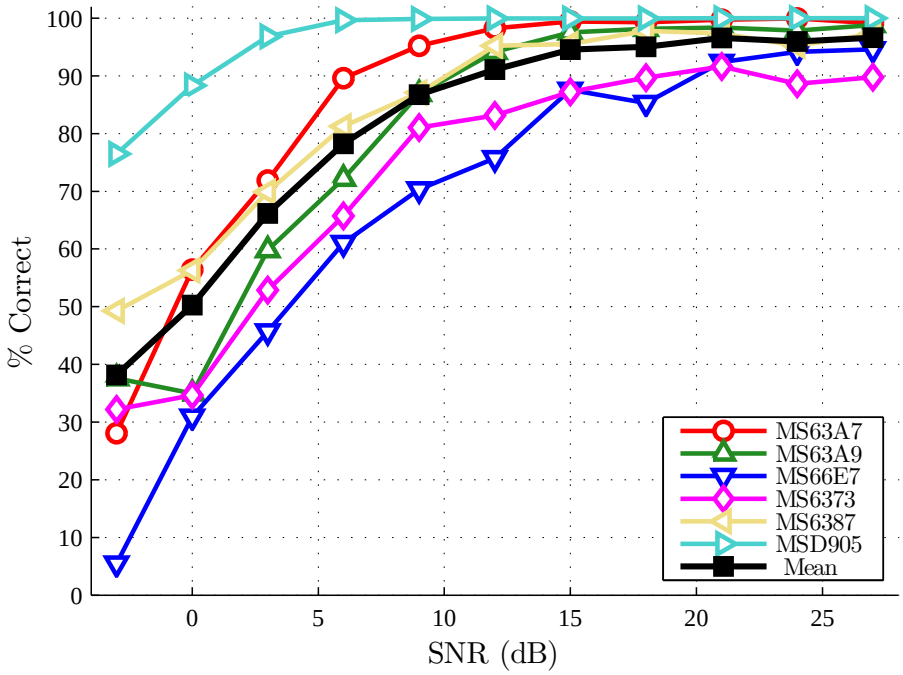
1. DRA Method #1: Individual WiMAX MS device *classification* performance using the DRA Method #1 feature subset–top 20 ranked features selected using relevance ranking at a single SNR, (3.17), is shown in Fig. 4.7. For $SNR \geq 15.0$ dB, individual device *classification* is 80% or better using the GRLQVI and MDA/ML classifiers. Average device *classification* is 90% or better for both classifiers at $SNR \geq 12.0$ dB.

2. DRA Method #2: Figure 4.8 shows individual WiMAX MS device *classification* performance using the DRA Method #2 feature selection technique–top 20 ranked features selected using the relevance rankings at each SNR, (3.18). Individual device *classification* is 80% or better using the GRLQVI and MDA/ML classifiers for $SNR \geq 15.0$ dB. These results are comparable to those of DRA Method #1.

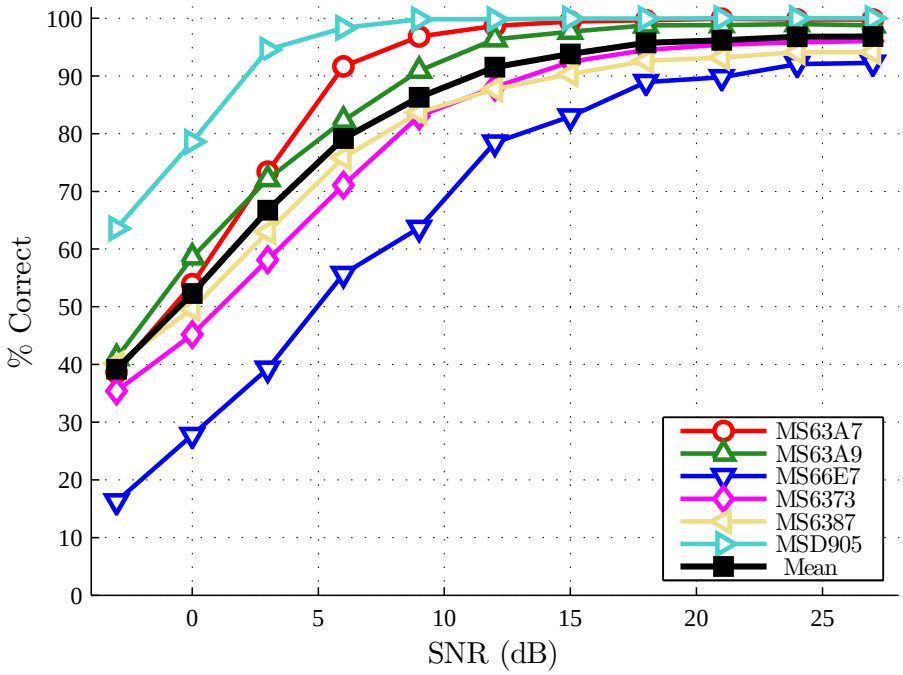
3. DRA Method #3: Figure 4.9 shows individual WiMAX MS device *classification* performance using the DRA Method #3 feature subset–top 20 ranked features are chosen from the average relevance ranking computed across all SNR, (3.19). Individual device *classification* is 80% or better for the GRLVQI classifier at $SNR \geq 15.0$ dB. The MDA/ML classifier achieves an individual device *classification* performance for five of the six MS of 80% or better for $SNR \geq 9.0$ dB. Unlike the previous two DRA methods, there are two notable observations from the DRA Method #3:

   (a) GRLQVI classifier performance is improved when compared with that of DRA Method #1 and Method #2.

   (b) MDA/ML performance is much better for five of the six MS devices than that of DRA Method #2.

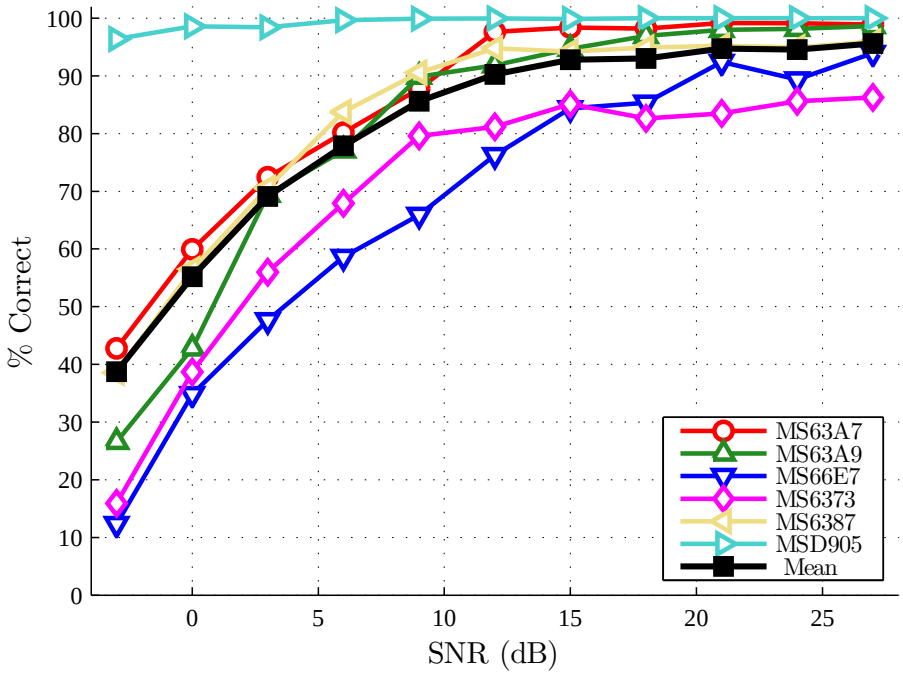


(a) GRLVQI Processing

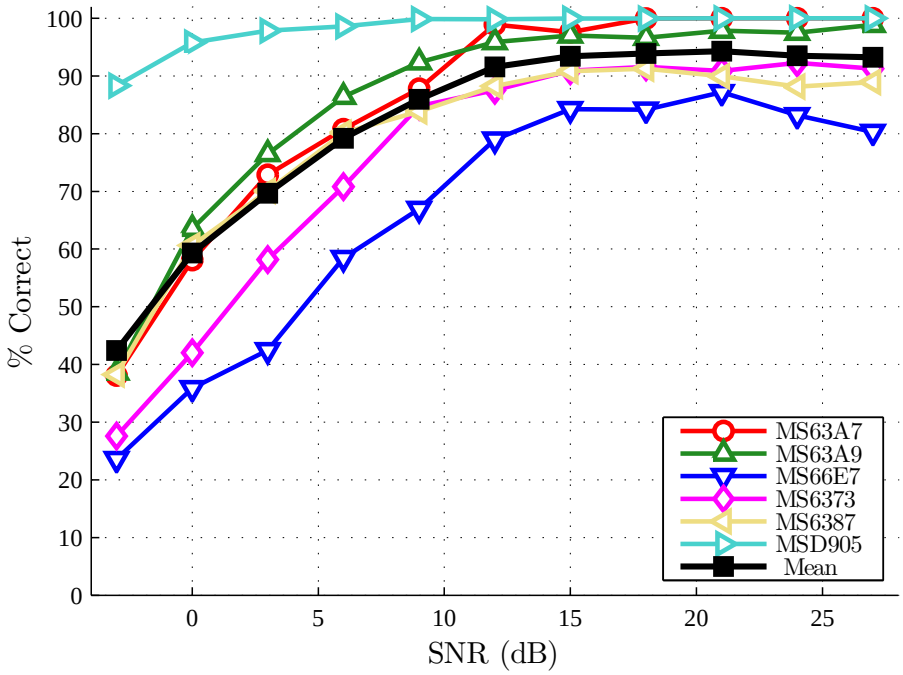


(b) MDA/ML Processing

Figure 4.7: *DRA Method #1*: Device *classification* performance with the top 20 ranked features selected by (3.17).



(a) GRLVQI Processing



(b) MDA/ML Processing

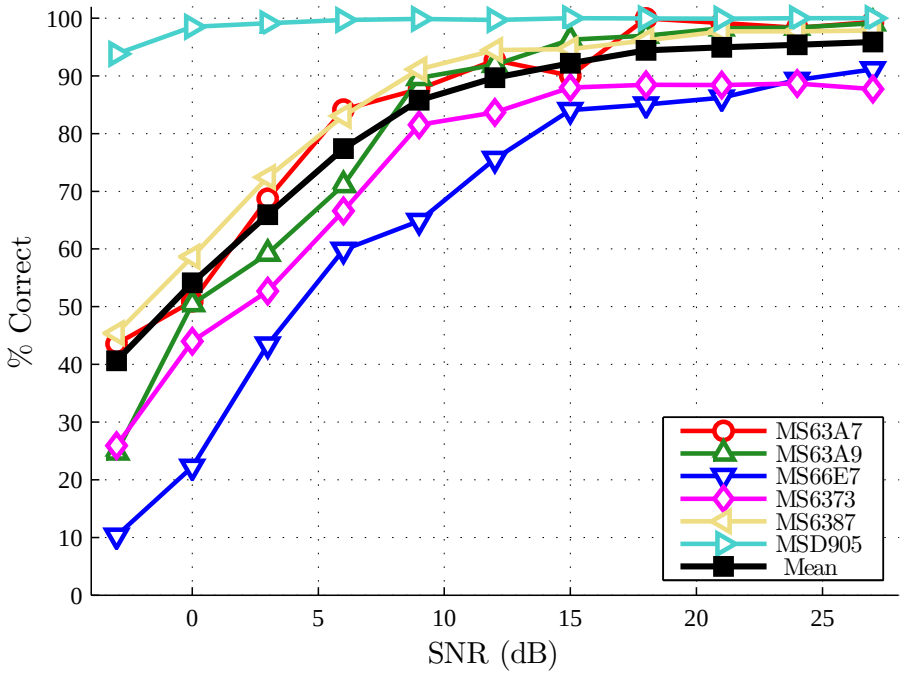
Figure 4.8: *DRA Method #2*: Device *classification* performance with top 20 ranked features selected using (3.18).

Observation: For operational network security, DRA Method #3 provides a means for determining a single, SNR independent set of features that can be used to discriminate devices under varying channel conditions. This simplifies system implementation and mitigates the need to estimate SNR in real-time applications.

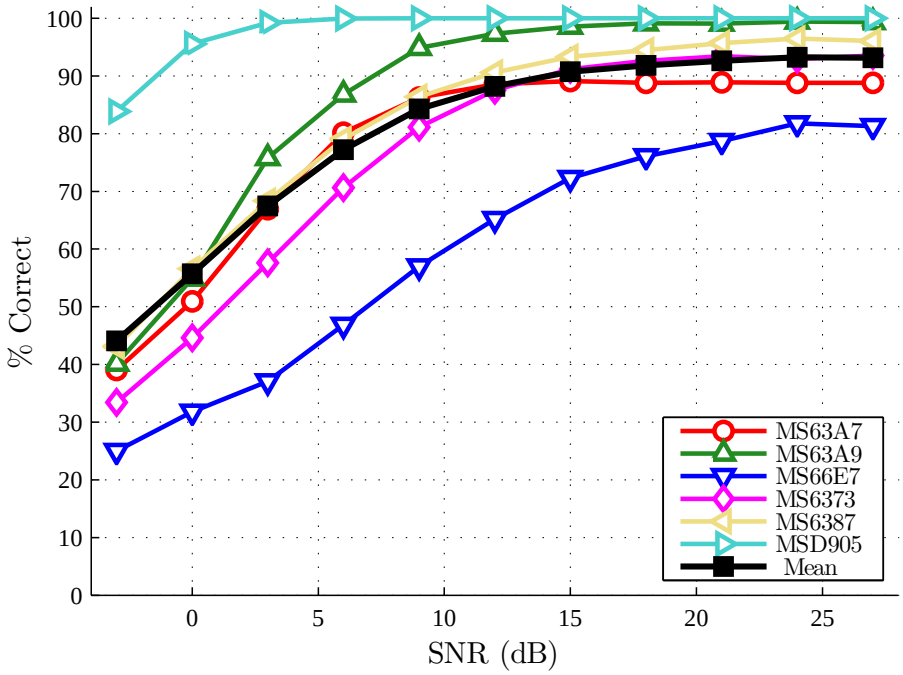
4. DRA Method #4: Individual WiMAX MS device *classification* performance using the DRA Method #4 feature subset is shown in Fig. 4.10 where the top 20 ranked features are selected the union of the relevance rankings across all SNR, (3.20). GRLVQI *classification* performance is 80% or better for all individual devices for $SNR \geq 15.0$ dB. When compared with DRA Method #3, GRLVQI performance is slightly degraded for MS6373 and MS66E7 for $SNR \geq 21.0$ dB. There is also a degradation of MDA/ML performance with respect to MS66E7 at $12 \geq SNR \leq 21.0$ dB. However, DRA Method #4 provides the same benefit as DRA Method #3 in that a single set of SNR independent features can be selected to provide device *classification*.

Figure 4.11 provides a direct comparison of average cross-device classification performance for a full-dimensional feature set and results for four DRA sets from Fig. 4.7 – Fig. 4.10. Figure 4.11(a) shows that GRLVQI processing with all four DRA selection methods yields average performance that is comparable to full-dimensional results. For MDA/ML processing, Fig. 4.11(b) shows that none of the DRA selection methods yield results matching full-dimensional performance, with 1) DRA Method #1 being superior to all other methods for $SNR \geq 15.0$ dB, and 2) all four DRA methods being within $\%C \approx \pm 5.0\%$ of one another for $SNR < 15.0$ dB. Based upon these results and the observation that DRA Method #3 provides a means for determining a single, SNR independent set of RF-DNA features, all subsequent DRA results are generated using reduced feature sets selected by DRA Method #3.

4.1.4 WiMAX Device ID Verification. For device ID *verification*, a total of twelve WiMAX MS devices are used. The six previously used for device *classification* are designated as "authorized" network devices and the remaining six MS

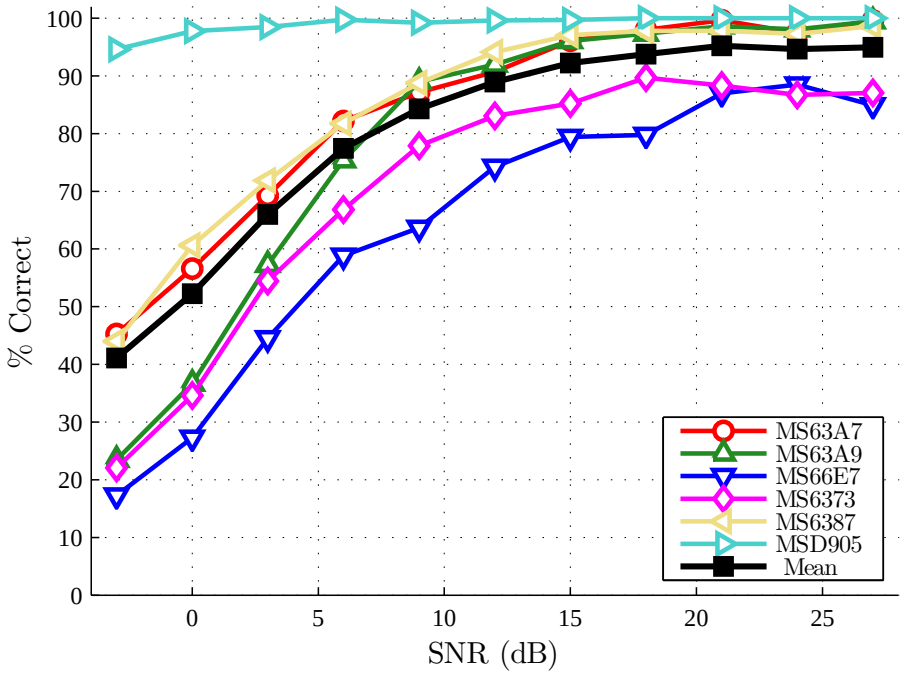


(a) GRLVQI Processing

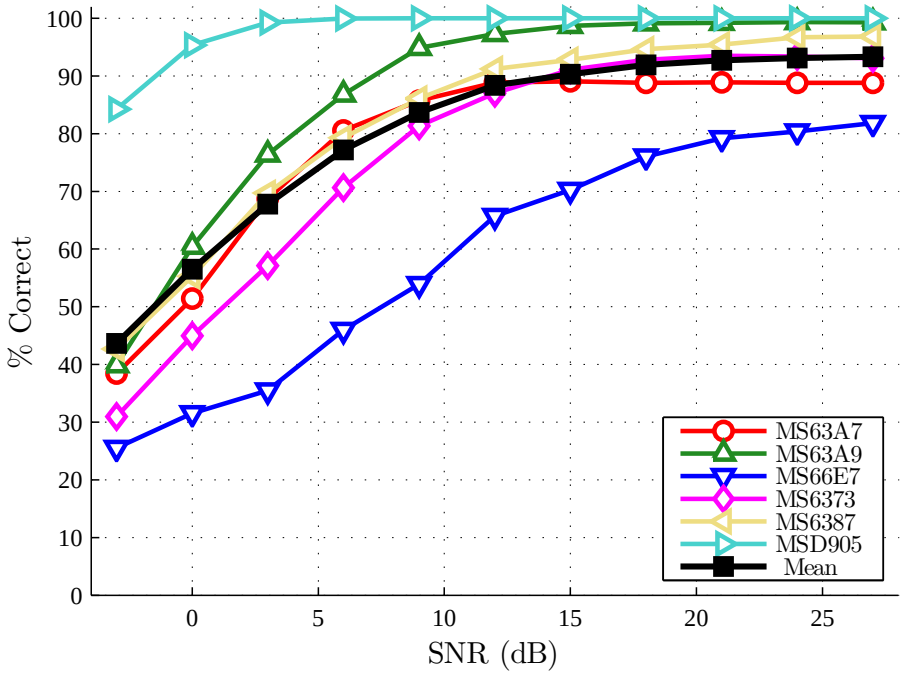


(b) MDA/ML Processing

Figure 4.9: *DRA Method #3*: Device *classification* performance with top 20 ranked feature selected using (3.19).

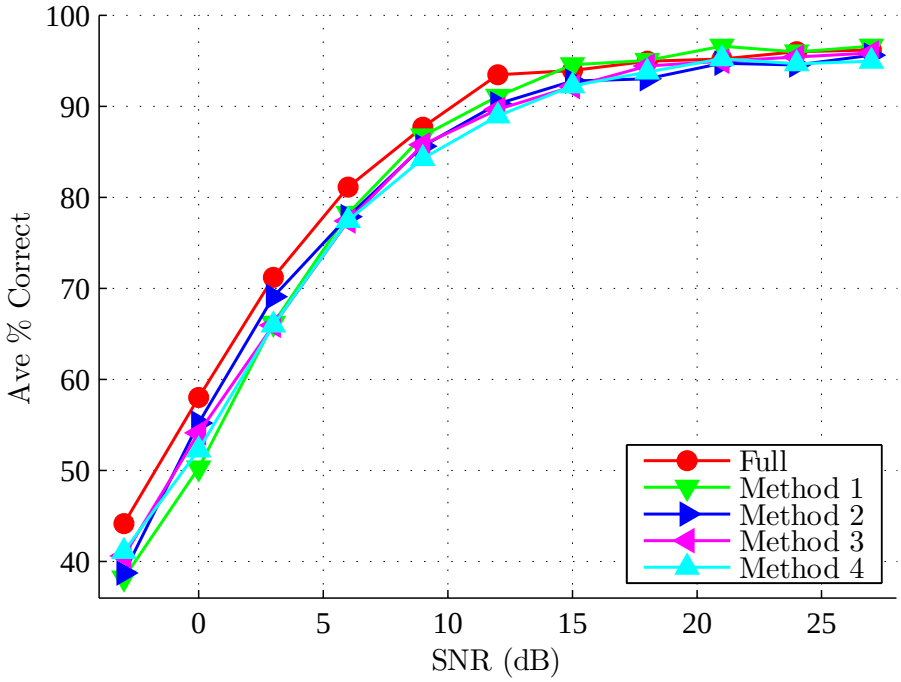


(a) GRLVQI Processing

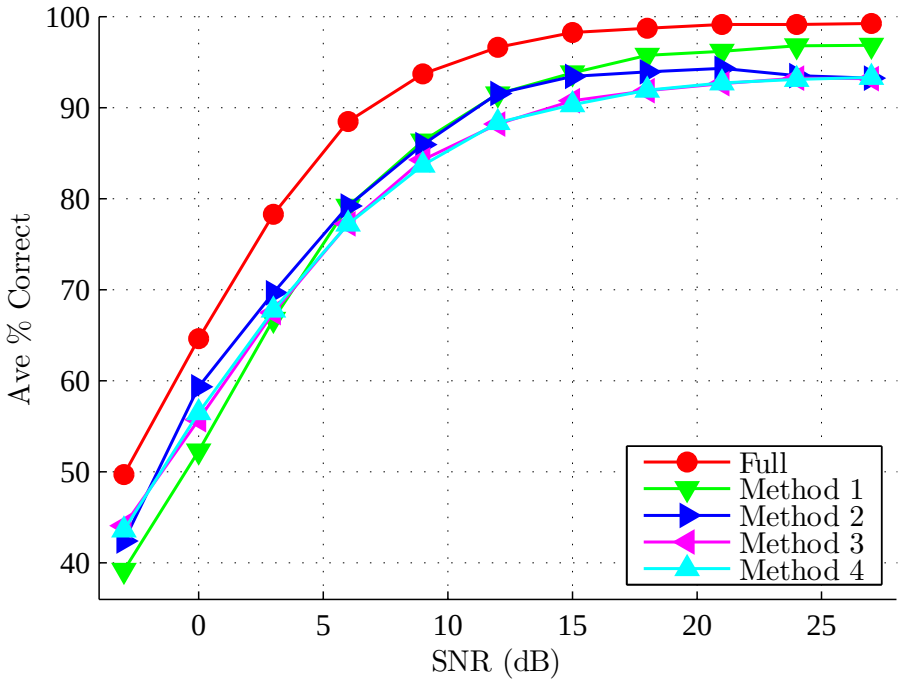


(b) MDA/ML Processing

Figure 4.10: *DRA Method #4*: Device *classification* performance with top 20 ranked feature selected using (3.20).



(a) GRLVQI Processing



(b) MDA/ML Processing

Figure 4.11: Overlay of average cross-device *Classification* performance for a full-dimensional feature set and results for four DRA sets from Fig. 4.7 – Fig. 4.10.

(ID #s MS637D, MS9993, MSC2FF, MSDAB9, MSDAC5, MSDDBF) are designated as "rogue" network devices. These "rogue" devices are used to assess device *verification* performance for the case where a previously unseen device (not present during classifier training) falsely presents a bit-level identity matching an authorized device and attempts to gain network access by posing as an authorized device.

4.1.4.1 MDA/ML Processing. As in [20, 29, 71], WiMAX device ID *verification* performance is assessed using full-dimensional GT RF-DNA fingerprints and the *Normalized Posterior Probability verification* test statistic z_v generated per (3.22) in Section 3.5.1. Individual *verification* performance for the six authorized WiMAX MS devices (ID #s MS63A7, MS63A9, MS66E7, MS6373, MS6387, MSD905) at SNR=6.0 dB is shown in Fig. 4.12. As described in Section 2.4 and Section 3.5.1, the ROC curves are formulated by testing the *verification* performance using each authorized device's *claimed* bit-level identity (MAC address) against their known *true* identity. This *true* identity is the "best" case model (minimum average *classification* error) resulting from the MDA/ML classifier training process. The individual ROC curves provide an illustration of the trade-off that exists between network security and receptiveness as the threshold t_v is varied for a selected device [20].

Figure 4.12 shows that for an arbitrary EER$\leq$10% benchmark is achieved for *all* six of the authorized devices. Devices MSD905 and MS66E7 achieved the highest and poorest EERs of 0% and 0.05% at SNR=6.0 dB, respectively. The ROC curves for the two WiMAX MS devices that resulted in the best case (Fig. 4.13(a)) and worst case (Fig. 4.13(b)) device *classification* performance for SNR=[0.0, 3.0, 6.0] dB are shown in Fig. 4.13. At SNR=0.0 dB, these figures show that the poorest EER occurs for MS66E7 with a value of approximately 0.23%. The *verification* results for the remaining four WiMAX MS devices (ID #s MS63A7, MS63A9, MS6373, MS6387) are shown in Fig. A.1 of Appendix A.1.

4.1.4.2 GRLVQI Processing. Based upon the results presented in Section 4.1.3, GRLVQI-based device ID *verification* is performed using dimensionally

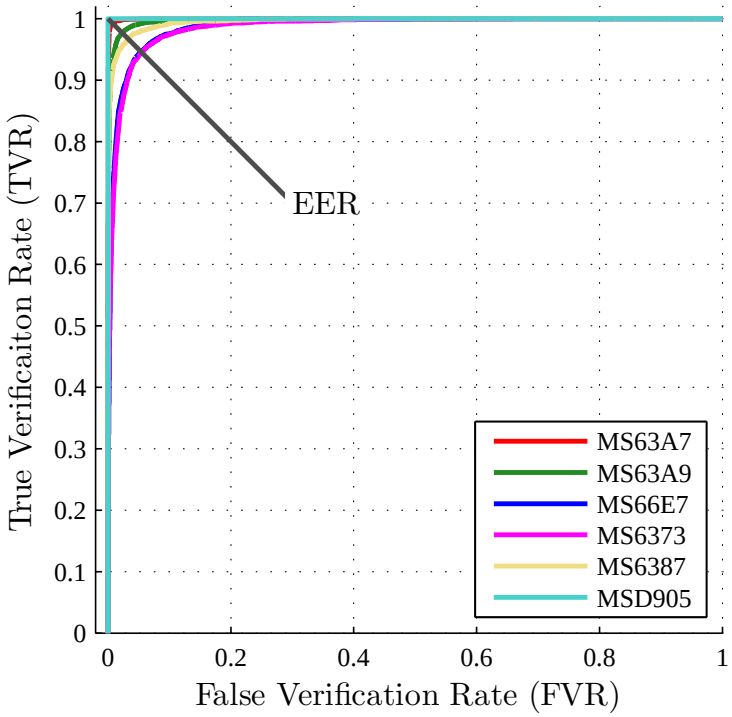
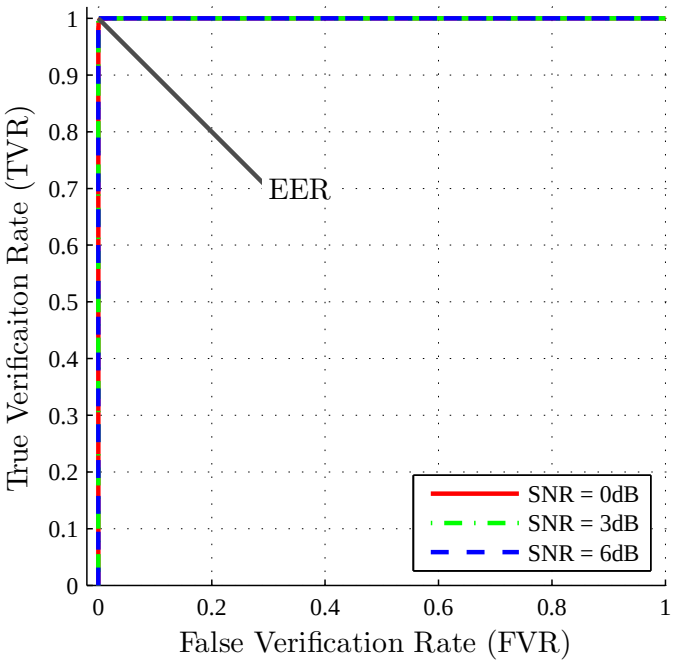


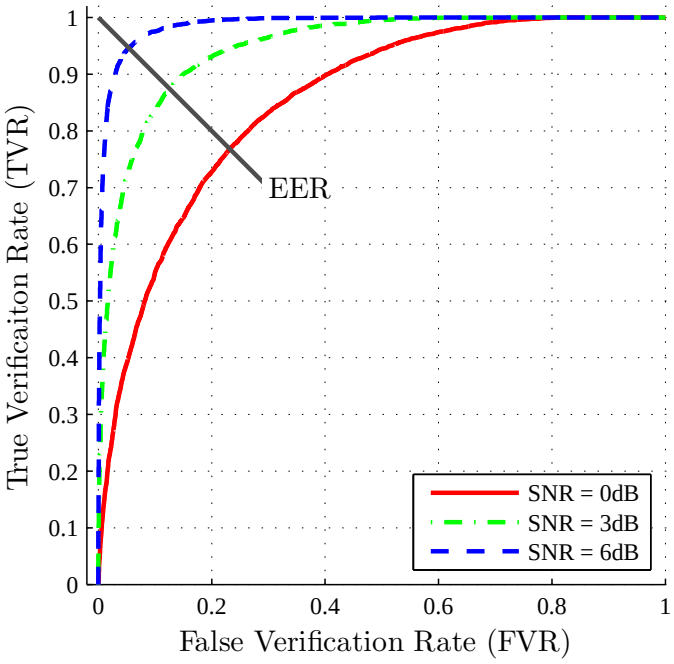
Figure 4.12: MDA/ML *verification* ROC curves for WiMAX MS devices using the *Normalized Posterior Probability* test statistic and Gabor Transform (GT) RF-DNA features at SNR=6.0 dB [71].

reduced GT RF-DNA Fingerprints in which the top 20 features are selected by DRA Method #4: (3.20). As with MDA/ML-based device ID *verification* results, presented in Section 4.1.4.1, ROC curves, created from the rates shown in Table 2.1 and an arbitrary benchmark of EER$\leq$10%, are used to quantify *verification* performance. In accordance with Section 3.5.2, the *verification* test statistic z_v is generated using one of four similarity measures, including: *Euclidean Distance* (d_E) per (2.29), *Normalized Euclidean Distance* ($\bar{d}_E$) per (3.27), *Spatial Angle* (θ_s) per (3.28), and *Spatial Angle-Times-Normalized Euclidean Distance* ($\theta_s \times \bar{d}_E$) per (3.29).

Device ID *verification* is performed using the set of N_C^A=6 *Authorized* WiMAX devices used for *classification* results presented at the beginning of Section 4.1. Figure 4.14 shows individual *Authorized* device *verification* performance using each of the four similarity measures. Results in Fig. 4.14(a) and Fig. 4.14(b) represent individual *Authorized* device *verification* performance using the distance-only d_E and



(a) Best Case: Device ID #MSD905.



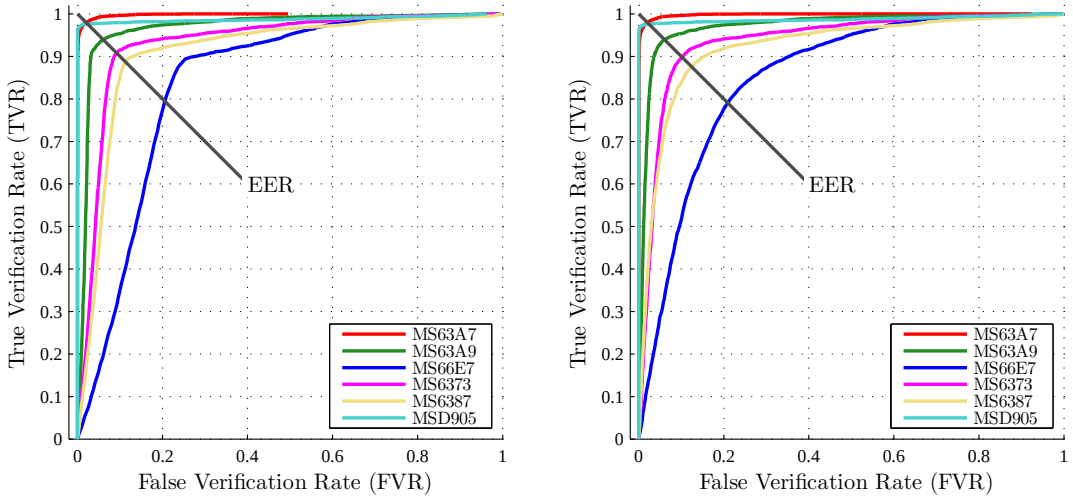
(b) Worst Case: Device ID #MS66E7.

Figure 4.13: MDA/ML *verification* ROC curves for best case and worst case WiMAX MS devices using the *Normalized Posterior Probability* test statistic and Gabor Transform (GT) RF-DNA features at SNR=[0.0, 3.0, 6.0] dB [71].

$\bar{d}_E$ test statistics, respectively. These two test statistics yielded poorest *Authorized* device *verification* performance and failed to achieve an arbitrary Authorized Device Verification Rate (ADVR) of ADVR≥90% (EER≤10%) for 2 of 6 authorized devices where ADVR equals the True Verification Rate (TVR) shown in the ROC curves. For both cases, poorest performance is indicated for authorized device ID #MS66E7 which would be denied network access nearly 20% of the time. In an effort to obtain the arbitrary EER≤10% benchmark for all authorized devices, *verification* is performed using test statistics generated from the *Spatial Angle* and the product of the *Spatial Angle* and *Normalized Euclidean Distance* similarity measure.

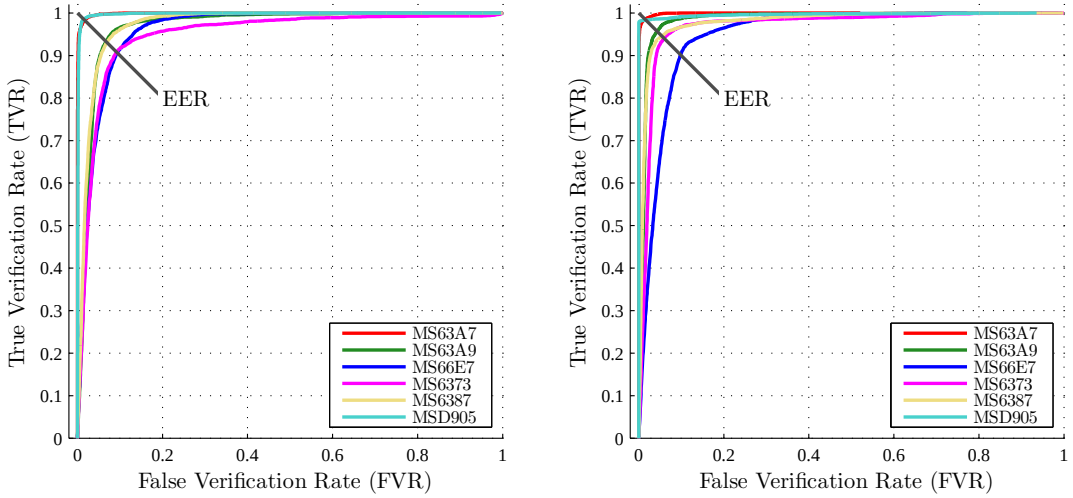
Results in Fig. 4.14(c) and Fig. 4.14(d) represent authorized device *verification* ROC curves using the spatial angle and product of the spatial angle and normalized Euclidean distance based test statistics. Both test statistics achieve the arbitrary EER≤10% benchmark for all six of the authorized devices. The product of the spatial angle and normalized Euclidean distance offers some improvement over spatial angle only in that 5 of the six devices achieves an EER≤0.10%.

The ability to verify *authorized* network devices only addresses one aspect of the network security problem. The other important aspect is the rogue device rejection capability. In this case, previously unseen "rogue" devices endeavor to gain unauthorized network access by posing as an *authorized* device. This is done by falsely presenting bit-level credentials matching an authorized device identity. This work has designated devices that perform such nefarious acts as *Rogue* devices. Therefore, an additional set of N_C^R=6 *Rogue* WiMAX devices (ID#s MS637D, MS9993, MSC2FF, MSDAB9, MSDAC5, MSDDBF) are used to test the effectiveness of the developed device ID *verification* process. Each of the N_C^R=6 *Rogue* WiMAX devices falsely presents the bit-level ID for each of the N_C^A=6 *Authorized* WiMAX devices; thus, representing a total of 36 attempts at gaining unauthorized network access. Of the six rogue devices, MS637D provided the greatest challenge to successful device *verification*. Figure 4.15 shows the *verification* results for the case of MS637D posing



(a) Euclidean Distance (d_E).

(b) Normalized Euclidean Distance ($\bar{d}_E$).



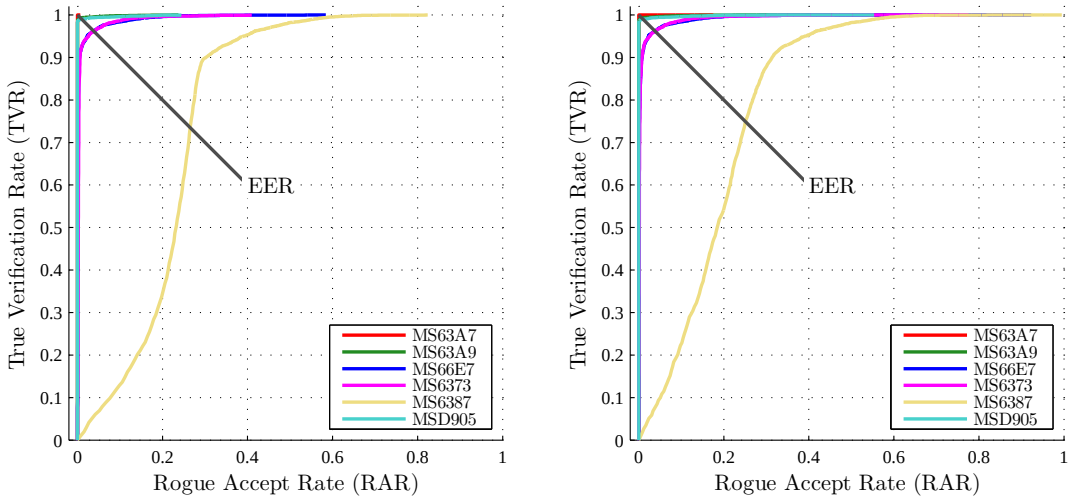
(c) Spatial Angle (θ_s).

(d) Angle-Times-Distance ($\theta_s \times \bar{d}_E$) [72].

Figure 4.14: GRLVQI *verification* ROC curves for N_C^A=6 *Authorized* WiMAX MS devices using Gabor Transform (GT) RF-DNA features at SNR=18.0 dB and indicated similarity measures per Section 3.5.2.

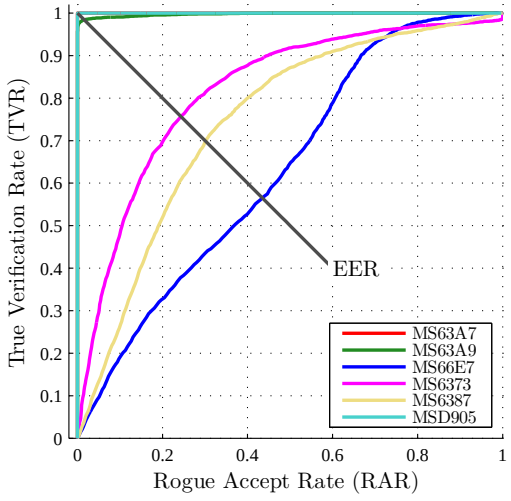
as each of the authorized devices. Results in Fig. 4.15(a) and Fig. 4.15(b) show that MS637D would gain network access approximately 25% of the time when claiming the bit-level identity of *authorized* device MS6387 and the *Euclidean* or *Normalized Euclidean* Distances are used as the test statistic z_v. Figure 4.15(c) illustrates that the *Spatial Angle* test statistic results in MS637D being verified as MS6373, MS6387, and MS66E7 at rates of approximately 25%, 30%, and 42%, respectively. This represents the poorest case of rogue device *verification*. Rogue device *verification*, for MS637D, based upon the product of spatial angle and normalized Euclidean distance is shown in Fig. 4.15(d). For this case, MS637D is verified as authorized device MS6387 approximately 30% of the time. When considering both *authorized* and *rogue* device *verification* performance, the product of the spatial angle and normalized Euclidean distance test statistic provides the best means of permitting authorized device access while simultaneously denying rogue devices. Using the angle-distance product, Fig. 4.16 shows resultant ROC and EER results representing a total of 36 rogue device detection scenarios where each of the N_C^R=6 *Rogue* devices present false bit-level credentials for each of the N_C^A=6 authorized devices. As indicated by the dashed line, *Rogue* device ID #MS637D provides the greatest security risk when presenting false bit-level credentials matching *authorized* device ID #MS6387 [72]. The remaining device *verification* results for all the test statistics and the remaining N_C^R=5 *Rogue* devices are presented in Appendix A.1.

Observation: The benefits of GT-based RF-fingerprints and DRA feature selection method #3 are leveraged for the 802.11a WiFi results.

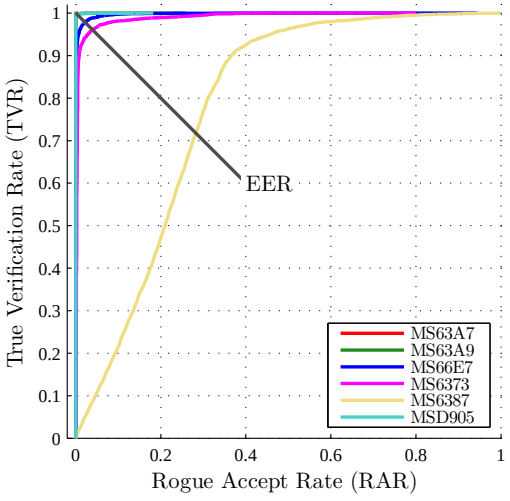


(a) Euclidean Distance (d_E).

(b) Normalized Euclidean Distance ($\bar{d}_E$).



(c) Spatial Angle (θ_s).



(d) Spatial Angle-Times-Normalized Euclidean Distance ($\theta_s \times \bar{d}_E$) [72].

Figure 4.15: GRLVQI *verification* ROC curves for N_C^R=6 *Rogue* WiMAX MS devices using Gabor Transform (GT) RF-DNA features at SNR=18.0 dB and indicated similarity measures per Section 3.5.2.

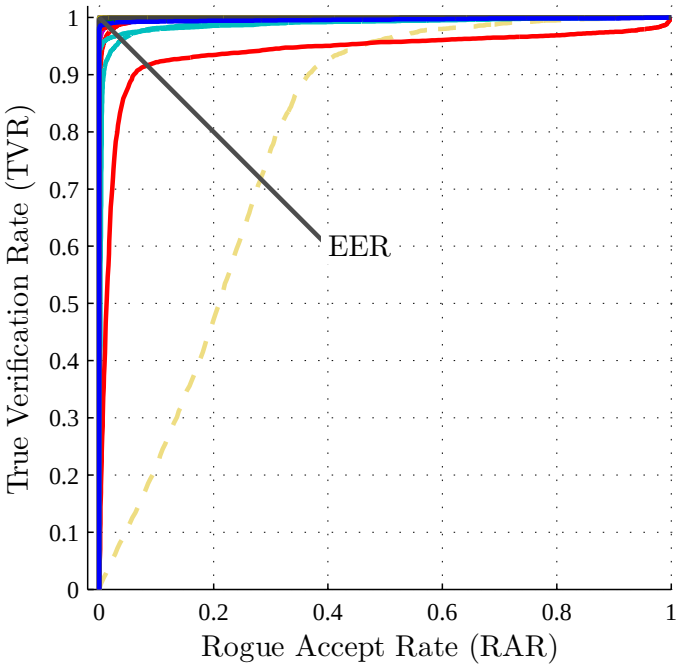


Figure 4.16: GRLVQI *verification* ROC curves for N_C^R=6 *Rogue* devices presenting false bit-level credentials for each of the N_C^A=6 authorized devices (36 total rogue scenarios represented) using Gabor Transform (GT) RF-DNA features at SNR=18.0 dB [72].

4.2 IEEE 802.11a WiFi Results

As described in Section 3.3 (*classification*) and Section 3.5 (*verification*), results were generated using RF-DNA fingerprints extracted from 802.11a WiFi preamble emissions–the same emissions used previously for Dual Tree Complex Wavelet Transform (DT-ℂWT) results in [56, 57]. Following the procedure outlined in Section 3.1, collections for each of the N_C=4 WiFi devices to ensure a total of N_B=1000 complex bursts per device. The collected signals were subsequently digitally filtered, individual bursts detected for removal from the overall collection record, and the SNR scaled per Section 3.2.

Assessment results in this section are for $SNR\in[-3.0, 27.0]$ dB in 3.0 dB increments, with the SNR scaling process was repeated N_z=10 times to ensure sufficient statistical significance for Monte Carlo analysis. For WiFi assessment, the full-dimensional TD, SD, GT, or GWT fingerprints were comprised of N_f=[117, 33, 363, 363].

Results are first presented for full-dimensional RF-DNA fingerprinting in Section 4.2.1 and Section 4.2.2 followed by reduced dimensional fingerprinting results in Section 4.2.3. As with WiMAX processing in Section 4.1, CI=95% confidence interval analysis was facilitated through the use of N_z=10 AWGN realizations per SNR with the intervals once again omitted in all data plots to enhance visual clarity.

WiFi device *classification* results are based on four like-model devices from the same manufacturer having different serial numbers–denoted herein as ID #s N4U9, N4UD, N4UW, N4PX; thus, representing serial number discrimination. Each of the RF-DNA fingerprint sets (TD, SD, GT, and GWT) was divided into two subsets. Training of the classifier and validation of the developed model is performed using the first subset. While the classifier is trained, the "best" reference model is selected and stored by tracking the model that results in the lowest *classification* error across all K=5 cross-validation folds and N_z=10 noise realizations. The second subset is used to perform a "blind" test of *classification* performance capability using the selected "best" reference model. Best practice pattern recognition processes suggest the use of such data partitioning techniques [48]. The "blind" test *classification* results are presented here using both full dimensional RF-DNA fingerprints in Section 4.2.1 and Section 4.2.2 while reduced dimensional RF-DNA fingerprints are presented in Section 4.2.3.

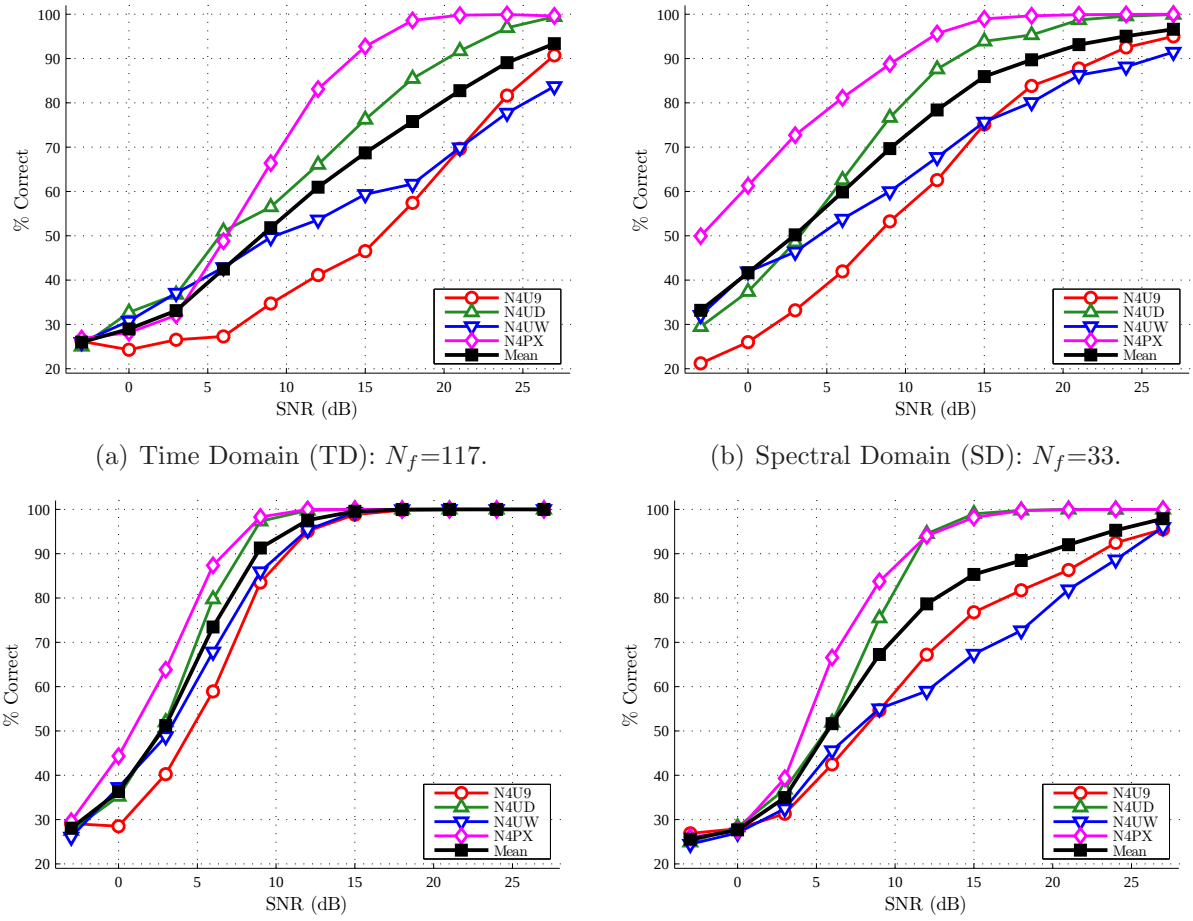
4.2.1 Full-Dimensional WiFi Classification: MDA/ML. MDA/ML *classification* results using the full-dimensional "blind" RF-DNA fingerprint subset are shown in this section. Individual device and average MDA/ML percent correct *classification* performance for all four RF-DNA fingerprint creation techniques, across $SNR \in [-3.0, 27.0]$ dB, are shown in Fig. 4.17. TD RF-DNA fingerprint results are shown in Fig. 4.17(a) and illustrates that average percent correct *classification* performance is 90% for SNR=27.0 dB. Individual device *classification* performance, using TD fingerprints, meets or exceeds 90% for 3 of the 4 investigated devices at the highest SNR. Individual MDA/ML *classification* performance, using SD RF-DNA, is 90%

or better for devices N4PX and N4UD at $SNR \geq 12.0$ dB, Fig. 4.17(b). Average SD RF-DNA *classification* performance is 90% or better at $SNR \geq 18.0$ dB. Joint time-frequency domain individual device and average *classification* performance is shown for GT and GWT RF-DNA fingerprints in Fig. 4.17(c) and Fig. 4.17(d), respectively. For GWT RF-DNA, only two of the four devices (ID #s N4UD, N4PX) achieve an individual *classification* percent correct performance of 90% or better at $SNR \geq 12.0$ dB, and average *classification* performance is 90% or better for $SNR \geq 21.0$ dB. Using GT RF-DNA fingerprints, the MDA/ML classifier obtains an individual device and average *classification* performance of 90% or better at $SNR \geq 12.0$ dB and $SNR = 9.0$ dB, respectively. These results show that GT−based RF-DNA fingerprinting provides the best means of achieving serial number discrimination of 802.11a WiFi devices.

Note: The superiority of GT fingerprinting in Fig. 4.17 is not attributable to the larger number of full-dimensional features being used. This is subsequently demonstrated using DRA in Section 4.2.3.

Figure 4.18 provides a comparison of the average MDA/ML *classification* performaces for each the four RF-DNA fingerprinting techniques described in Section 2.2 as well as the DT-ℂWT results from [56, 57]. The DT-ℂWT results are for the same four 802.11a WiFi devices and are the average computed across all combinations of three devices. Each of the DT-ℂWT RF-DNA fingerprints were comprised of $N_f = 135$ features. The GT−based *classification* results are superior to the DT-ℂWT results, for $SNR \geq 4.0$ dB. Relative to other features, GT RF-DNA fingerprinting yields a gain in performance of $G_p \approx 16.0$ dB (TD), $G_p \approx 9.0$ dB (SD), $G_p \approx 9.0$ dB (GWT), and $G_p \approx 7.0$ dB (DT-ℂWT) at %C=90% *classification* accuracy. As in [94], SD RF-DNA fingerprinting performance is consistent with DT-ℂWT performance across all investigated SNR.

4.2.2 Full-Dimensional WiFi Classification: GRLVQI. Using the same RF-DNA fingerprints for four WiFi devices classified in Section 4.2.1, full-dimensional GR-LVQI *classification* results are presented in this section. Figure 4.19 illustrates indi-



(a) Time Domain (TD): N_f=117.

(b) Spectral Domain (SD): N_f=33.

(c) Gabor Transform (GT): N_f=363.

(d) Gabor-Wigner Transform (GWT): N_f=363.

Figure 4.17: Full-Dimensional MDA/ML *classification* performance using TD, SD, GT and GWT RF-DNA features from N_C=4 802.11a WiFi devices.

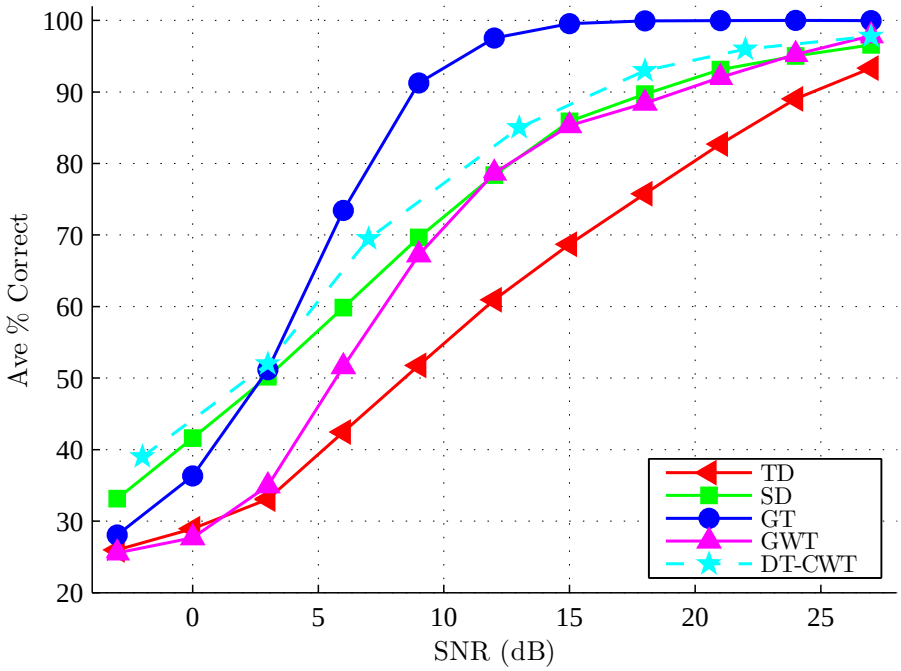
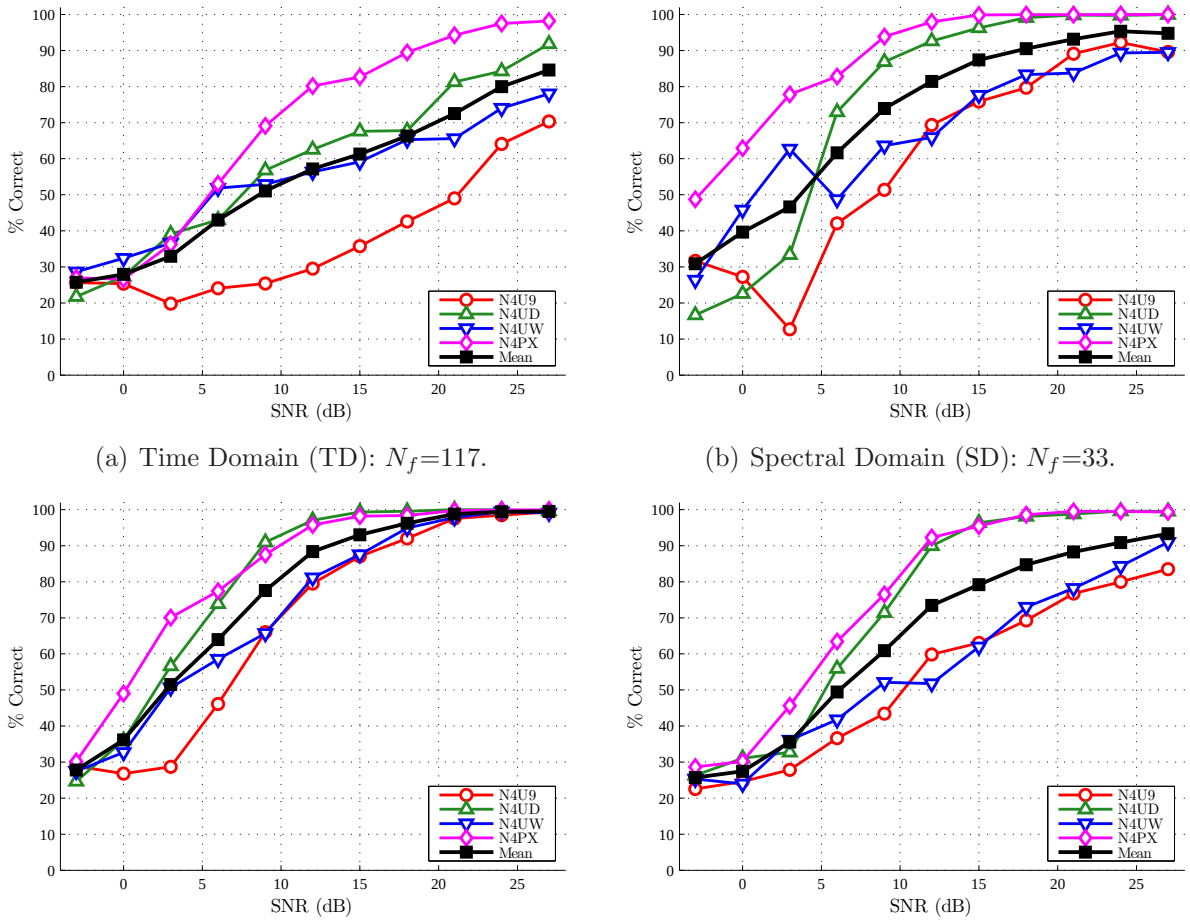


Figure 4.18: Average MDA/ML WiFi *classification* performance from Fig. 4.17 overlayed with previously published DT-ℂWT results from [57].

vidual device and average GRLVQI percent correct *classification* performance for TD, SD, GT, and GWT RF-DNA fingerprint generation techniques at $SNR \in [-3.0, 27.0]$ dB. Figure 4.19(a) shows individual device and average GRLVQI percent correct *classification* performance using TD RF-DNA fingerprints. Average TD RF-DNA *classification* fails to achieve the 90% correct performance benchmark for all investigated SNR, and only device N4PX is classified correctly at a rate of 90% or better for $SNR \geq 18.0$ dB. GRLVQI individual device and average *classification* results, using SD fingerprints, are shown in Fig. 4.19(b). Two of the tested 802.11a WiFi devices (ID #s N4UD and N4PX) are correctly classified at a rate of 90% or better for $SNR \geq 12.0$ dB. Average *classification* performance using SD RF-DNA is 90% or better for $SNR \geq 18.0$ dB and represents a significant, approximate 18.0 dB improvement over TD results.

GT-based RF-DNA fingerprint GRLVQI *classification* performance is illustrated in Fig. 4.19(c). All four devices are correctly classified at 90% or better performance for $SNR \geq 18.0$ dB. Average percent correct *classification* performance meets or



(a) Time Domain (TD): N_f=117.

(b) Spectral Domain (SD): N_f=33.

(c) Gabor Transform (GT): N_f=363 [73].

(d) Gabor-Wigner Transform (GWT): N_f=363.

Figure 4.19: Full-Dimensional GRLVQI *classification* performance using TD, SD, GT and GWT RF-DNA features from N_C=4 802.11a WiFi devices.

exceeds the arbitrary 90% benchmark for $SNR \geq 15.0$ dB. GRLVQI individual device and average percent correct *classification* performance is illustrated in Fig. 4.19(d) for the GWT RF-DNA generation technique. As with GT-based results, GWT-based RF-DNA *classification* performance of WiFi devices: N4UD and N4PX, is 90% or better for $SNR \geq 12.0$ dB. However, when comparing average GWT RF-DNA *classification* performance to that of the GT-based results, performance is deteriorated by approximately 9.0 dB. As with MDA/ML results in Section 4.2.1, GRLVQI *classification* using GT RF-DNA fingerprints provides the best means for achieving serial number discrimination of 802.11a WiFi devices. This is illustrated in Fig. 4.20 results which reflect an approximate gain of G_p=15.0 dB (TD), G_p=5.0 dB (SD), and G_p=10.0 dB (GWT-based) for other methods.

Note: The superiority of GT fingerprinting in Fig. 4.19 is not attributable to the larger number of full-dimensional features being used. This is subsequently demonstrated using DRA in Section 4.2.3.

A direct comparison of average *classification* performance, using GT RF-DNA, of the MDA/ML and GRLVQI classifiers is shown in Fig. 4.21. The MDA/ML and GRLVQI average performances are statistically equivalent for $SNR \in [-3.0, 3.0]$ dB and $[21.0, 27.0]$ dB. MDA/ML average results are superior to GRLVQI-based results for $SNR \in [3.0, 21.0]$ dB; however, at the point of greatest difference ($SNR \approx 9.0$ dB) GRLVQI is within 12% of MDA/ML classifier performance. As previously stated, the advantage, over MDA/ML, of the GRLVQI classifier is that it facilitates Dimensionality Reduction Analysis by providing a measure of feature contribution to a *classification* decision, via the relevance ranking λ_i.

4.2.3 DRA Impact on WiFi Classification. Based upon WiFi *classification* results in Section 4.2.1 and Section 4.2.2 along with the WiMAX results in Section 4.1.3, the impact of dimensionally reduced WiFi GT RF-DNA fingerprints on MDA/ML and GRLVQI classifier performance was next assessed. Based on the initial WiMAX DRA assessment in Section 4.1.3, it was determined that a feature

set containing only the top 10% of ranked features provided statistically equivalent *classification* performance to results achieved using a full-dimensional feature set. Furthermore, selection of the DRA feature subset was performed using DRA Method #3 for the following reasons:

1. GRLQVI classifier performance was best when using DRA Method #3 when compared to performance using either DRA Method #1 and Method #2.
2. MDA/ML classifier performance was much better for five of six MS devices when using DRA Method #3 relative to what was achieved using Method #2.
3. DRA Method #3 provides a means for determining a single, SNR independent subset of relevant features that can be used to reliably discriminate devices at multiple SNR; this mitigates the need to estimate SNR in real-time applications and enhances experimental-to-operational transition opportunity.

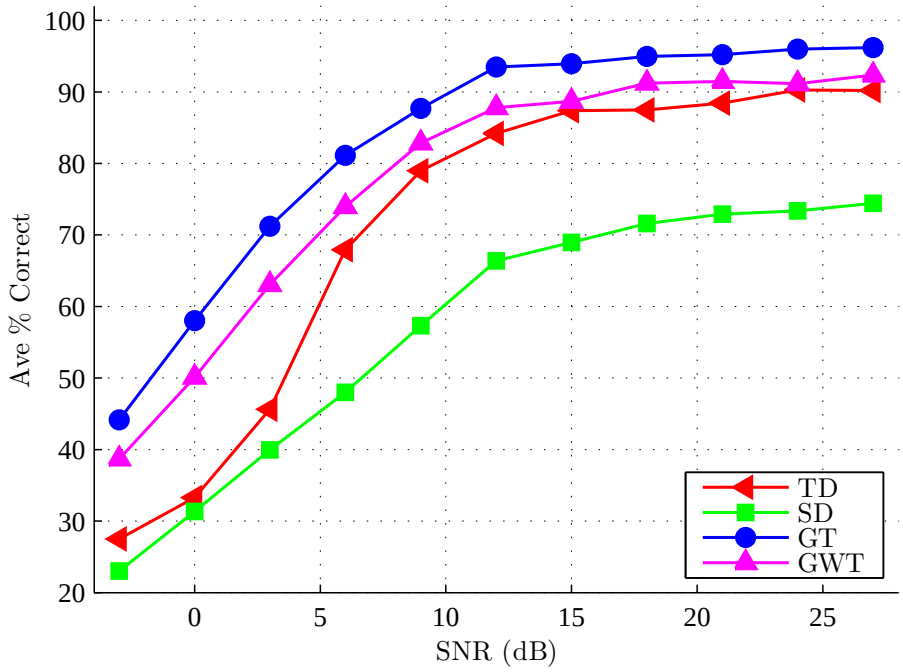


Figure 4.20: Average GRLVQI *classification* performances from Fig. 4.19 using TD, SD, GT and GWT RF-DNA features from N_C=4 802.11a WiFi devices.

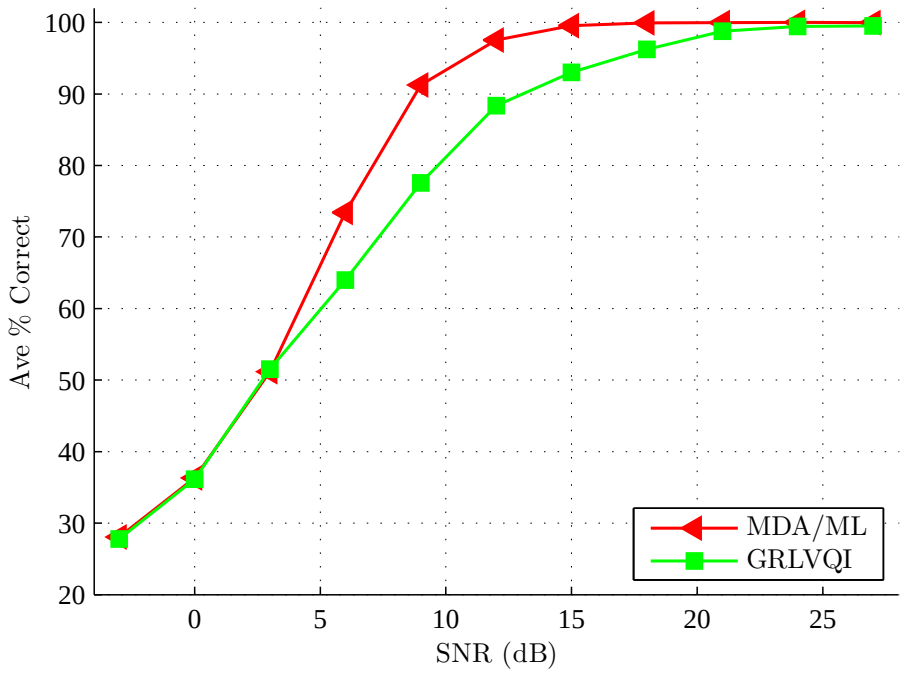


Figure 4.21: WiFi classifier performance comparison showing Fig. 4.18 MDA/ML and Fig. 4.20 GRLVQI cross-device average results using Gabor Transform (GT) RF-DNA features from N_C=4 802.11a WiFi devices.

Figure 4.22 shows T-F responses for arbitrary bursts that were randomly selected from each of the N_C=4 802.11a WiFi devices (ID #s N4U9, N4UD, N4UW, N4PX). The regions containing the highest ranked 10% (Top 36) features are highlighted by red rectangles. All reduced dimensional results in this section were generated using the highest ranked N_f=36 WiFi features.

Figure 4.23 shows WiFi device *classification* performance using the top N_f=36 ranked GT features that were selected using DRA Method #3 per (3.19). As shown, MDA/ML performance is generally better than GRLVQI using the dimensionally reduced GT RF-DNA fingerprints and includes: 1) all four WiFi devices achieving the %C≥90% benchmark at SNR≥12.0 dB (SNR≥16.0 dB for GRLVQI), and 2) cross-device average performance of %C≥90% for SNR≥10.0 dB (SNR≥12.0 dB for GRLVQI). The MDA/ML and GRLVQI cross-device averages are shown overlaid in Fig. 4.24 to enable direct comparison. By comparison with full-dimensional results in Section 4.2.1 and Section 4.2.2, both methods reflect an approximate 3.0 dB per-

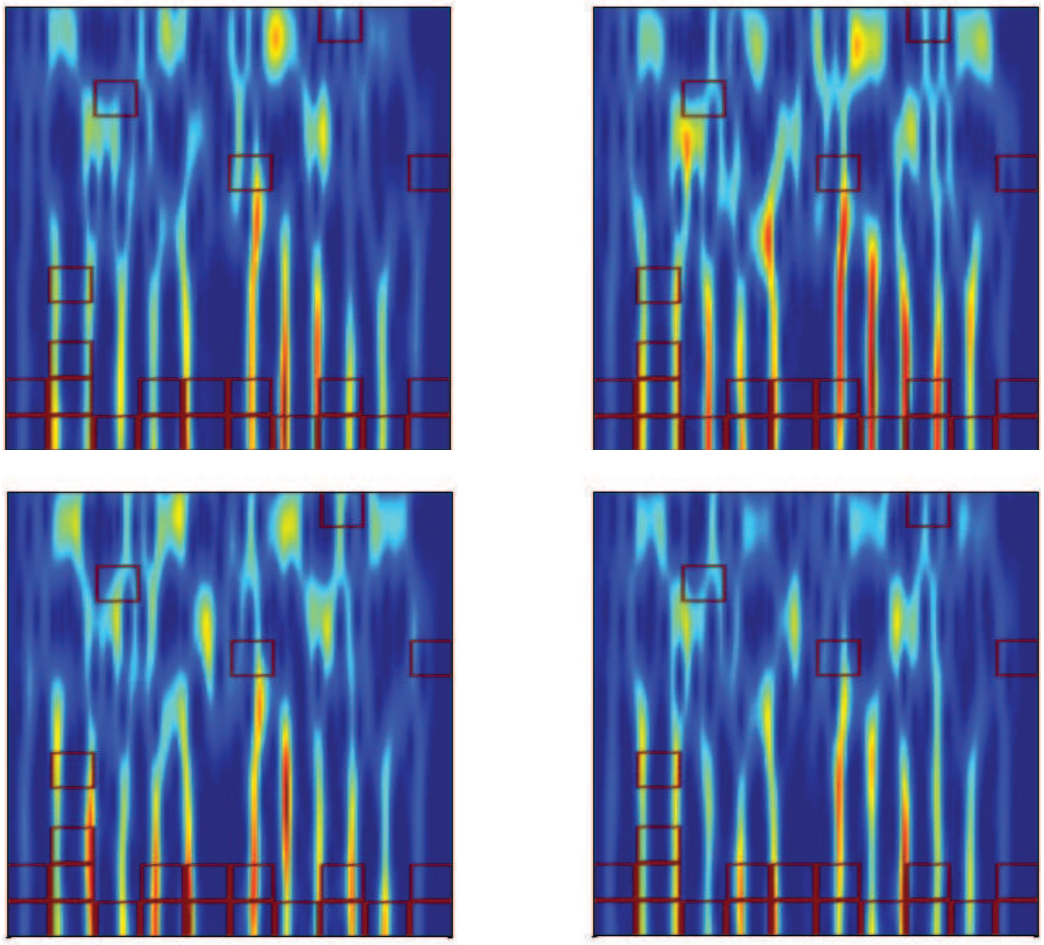
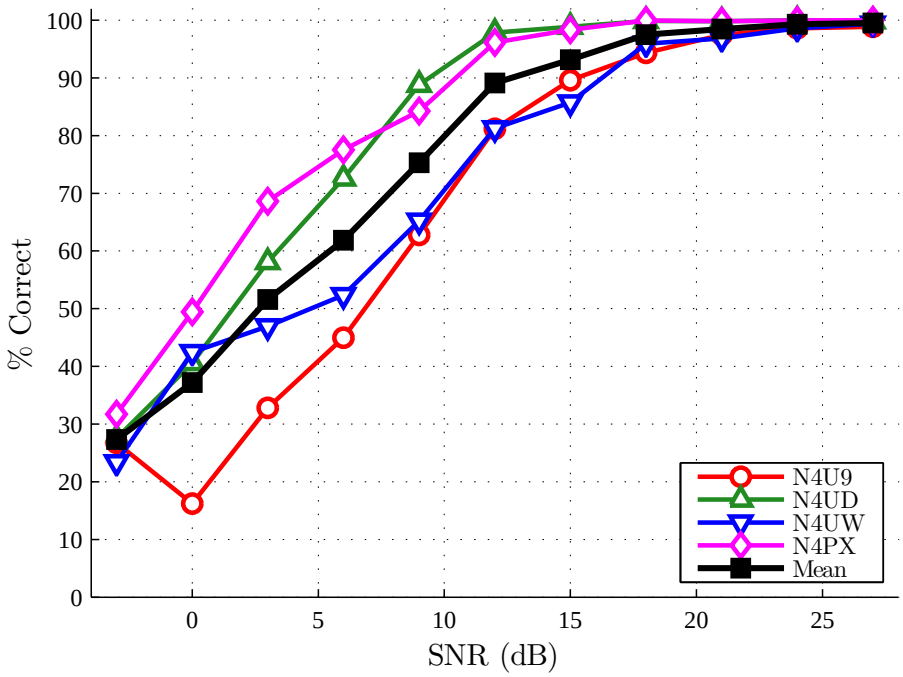


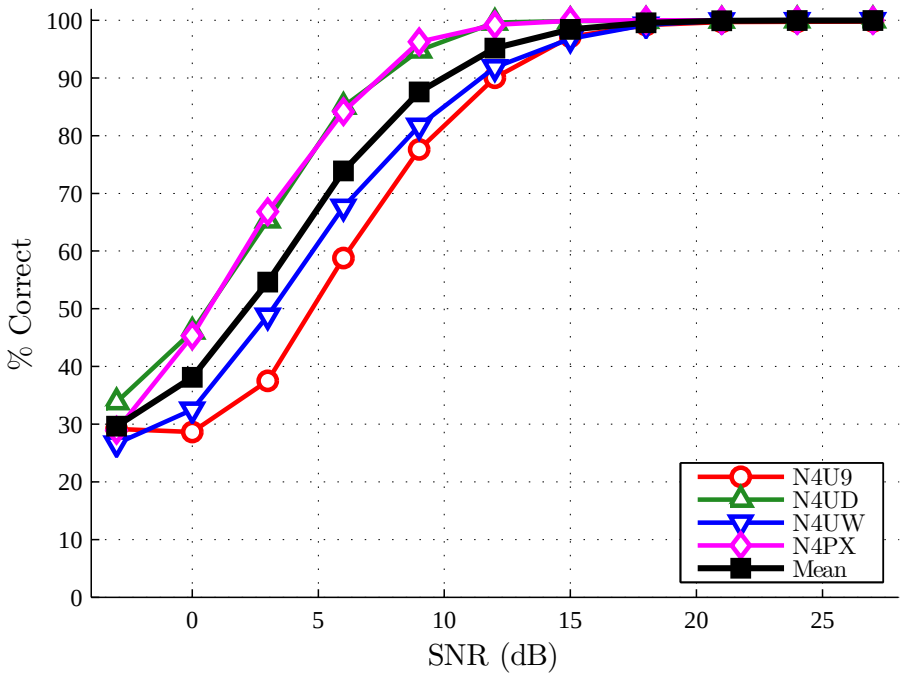
Figure 4.22: Gabor T-F responses for N_C=4 WiFi devices: Rectangular patches identify regions containing the highest ranked 10% (Top 36) features. One representative response shown per device [73].

formance degradation using DRA; however, the dimensionally reduced results only required approximately *one-tenth* the original computation time.

4.2.4 WiFi Device ID Verification. Device ID *verification* results are presented for the four 802.11a WiFi devices (ID #s N4U9, N4UD, N4UW, N4PX) using dimensionally reduced GT fingerprints. The features were ranked and selected using DRA Method #3 and the device ID *verification* process implemented per Section 3.5.2. Figure 4.25 shows *verification* ROC curves in which the arbitrary EER$\leq$10% benchmark is met or exceeded for all N_C^A=4 *Authorized* WiFi devices at SNR=15.0 dB. Devices N4UD and N4U9 provided best and worst case performance of EER$\approx$0.009% and EER$\approx$0.101%, respectively. Figure 4.26 shows the ROC curves associated with the WiFi devices that resulted in the best (Fig. 4.26(a)) and worst (Fig. 4.26(b)) case individual *classification* performance for SNR=[12.0, 15.0, 18.0] dB. The poorest performance is associated with WiFi device N4U9 which resulted in EER$\approx$0.2% at SNR=12.0 dB. Additional results for the N4UW and N4PX WiFi devices at SNR=[12.0, 15.0, 18.0] dB are presented in Fig. A.22 of Appendix A.2.



(a) GRLVQI Processing [73]



(b) MDA/ML Processing

Figure 4.23: WiFi GRLVQI and MDA/ML *classification* performance for N_C=4 devices using the Top 36 features selected with *DRA Method #3* per (3.19).

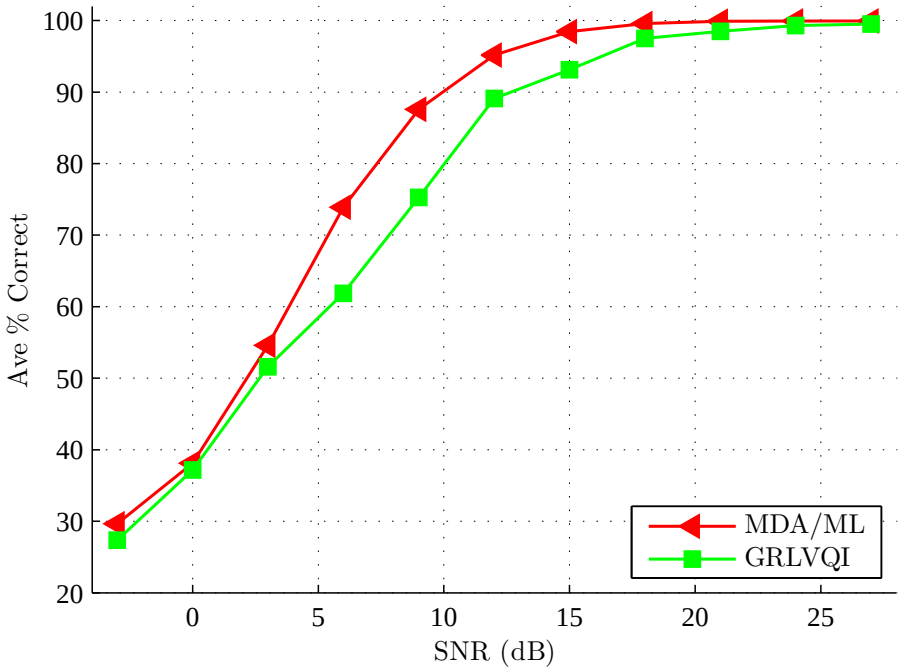


Figure 4.24: Overlay of GRLVQI and MDA/ML average cross-device 802.11a WiFi performances from Fig. 4.23. Results for GT RF-DNA features for N_C=4 devices using the Top 36 features selected with *DRA Method #3* per (3.19).

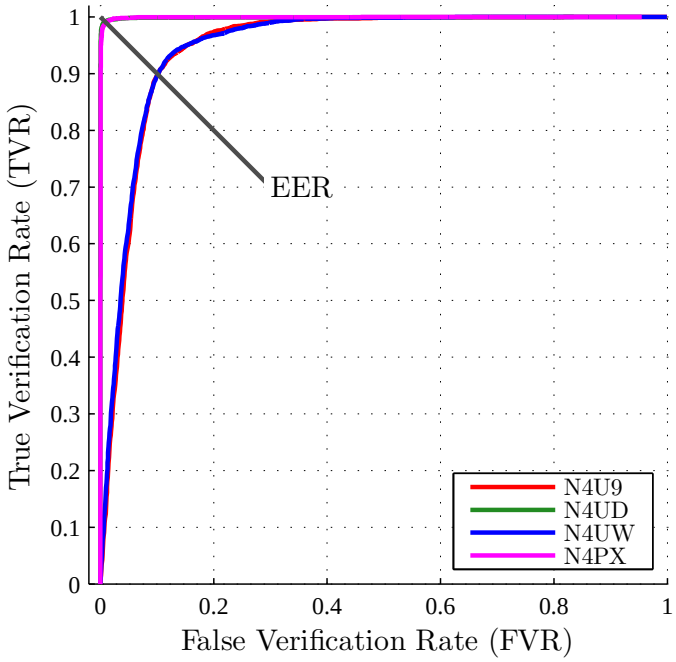
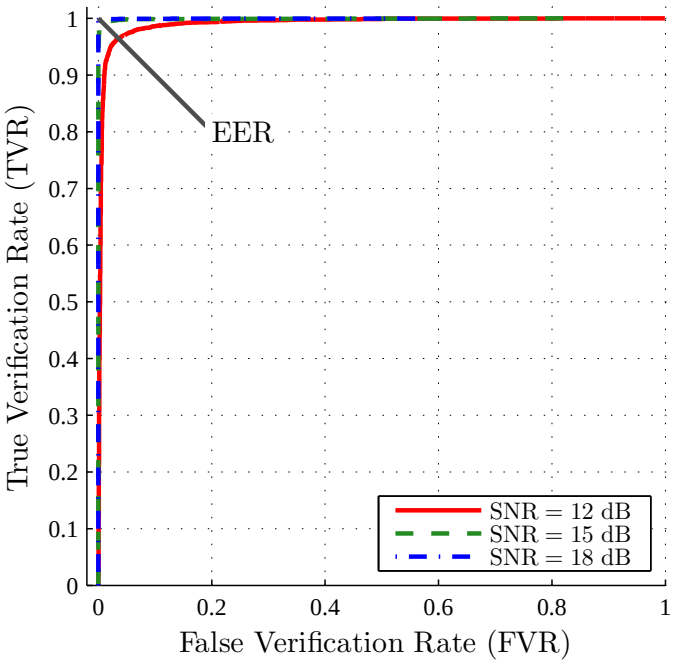
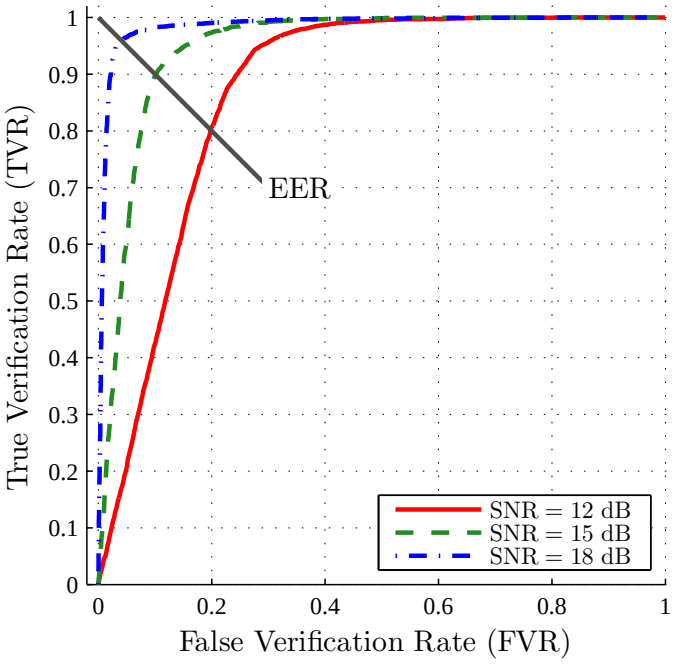


Figure 4.25: GRLVQI *verification* ROC curves for N_C^A=4 *Authorized* WiFi devices using a dimensionally reduced (top 36) Gabor Transform (GT) RF-DNA feature set at SNR=15.0 dB [73].



(a) Best Case: Device ID #N4UD.



(b) Worst Case: Device ID #N4U9.

Figure 4.26: GRLVQI *verification* ROC curves for best case and worst case WiFi devices using a reduced dimensional Gabor Transform (GT) RF-DNA feature set at SNR=[12.0, 15.0, 18.0] dB [73].

4.3 Multipath Impact on Classification

Results are presented here for a "first-look" investigation into the impact of multipath on device *classification* performance. For this investigation, 802.11a WiFi preamble responses were used given that 1) a considerable amount of previous research has been completed using the 8012.11a signal [54, 56, 57, 67, 73, 81, 82, 84, 94], and 2) a comparative performance baseline was established in Section 4.2. Based on results in Fig. 4.17 and Fig. 4.19, RF-DNA fingerprints were generated from both GT and GWT T-F responses of 802.11a WiFi preambles using the process outlined in Section 2.2.3. Use of GT and GWT features facilitated the analysis of both linear (GT) and non-linear (GWT) transform effects on device *classification* in the presence of multipath.

Motivation: The technical community encouraged consideration of non-linear feature transforms and suggested that such transforms may provide greater robustness under multipath conditions.

A Rayleigh faded channel was considered for the initial assessment of multipath impact on device *classification*. As illustrated in Fig. 4.27, the channel was modeled as including the direct path Line-of-Sight (LOS) signal $\mathbf{s}_{LOS}$ and a single stationary reflector producing the reflected signal $\mathbf{s}_{REF}$. Samples of the composite received multipath signal ($\mathbf{s}_{MP}$) are given by,

$$\mathbf{s}_{MP}[k] = \mathbf{s}_{LOS}[k] + \mathbf{s}_{REF}[k] + \mathbf{n}_b[k], \tag{4.1}$$

where $\mathbf{n}_b[k]$ are independent background noise samples and

$$\mathbf{s}_{REF}[k] = A_R \mathbf{s}_{LOS}[k - k_R], \tag{4.2}$$

with A_R (amplitude) and k_R (delay) being random channel control parameters.

The Rayleigh fading channel parameters were configured such that the reflected signal $\mathbf{s}_{REF}$ had 1) one-half the power of direct LOS signal $\mathbf{s}_{LOS}$, and 2) an average time delay of $k_R \approx 0.2$ μs. The desired channel effects were achieved using

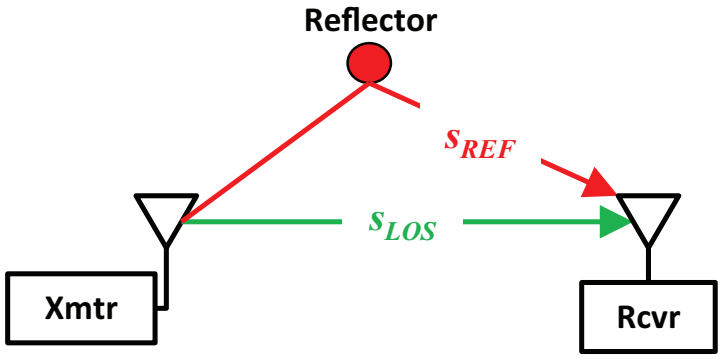
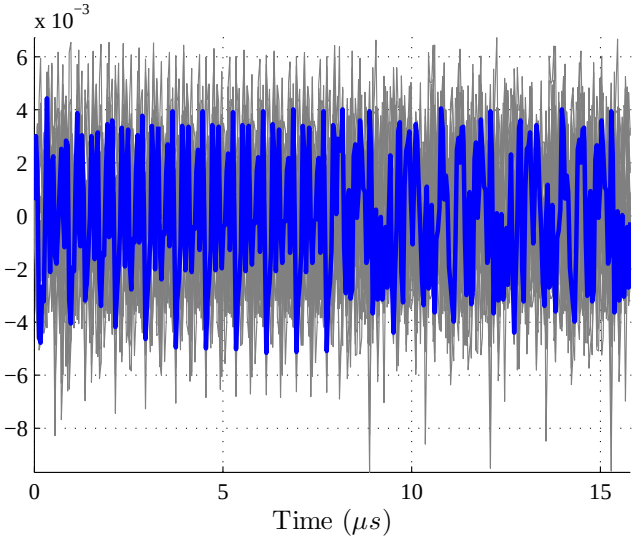


Figure 4.27: Rayleigh faded multipath channel implemented with a direct path LOS signal s_{LOS} and a reflected response s_{REF} using Matlab® 's *rayleighchan.m* function.

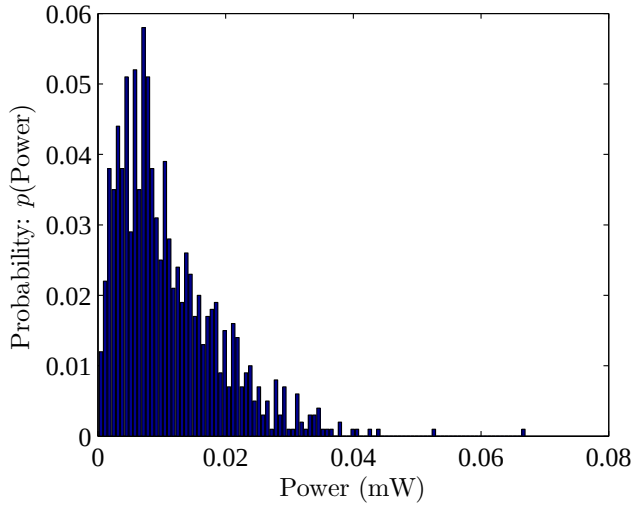
Matlab® 's *rayleighchan.m* function to create the multipath model. To characterize the *rayleighchan.m* function performance prior to using it for multipath assessment, the function was called 1000 times and each resultant channel model convolved with the same randomly selected 802.11a WiFi burst response. Figure 4.28(a) shows the selected LOS s_{LOS} burst response overlayed with 25 s_{MP} multipath signal responses. Figure 4.28(b) shows the Probability Mass Function (PMF) of the estimated signal power for each of the received signals and clearly shows the Rayleigh fading effect due to the generated multipath channel.

Device *classification* under multipath conditions was performed using the MDA-/ML classifier described in Section 2.3.1 and Section 3.3.1. As summarized in Table 4.1, there were three device *classification* scenarios considered, including:

1. Both model development (classifier training) and *classification* are performed using RF-DNA extracted from signal responses with ***no multipath present*** (M1, T1),
2. Model development using RF-DNA extracted from responses with ***no multipath present*** and subsequent *classification* using RF-DNA extracted from signal responses with ***multipath present***, (M1, T2), and



(a) Overlay of direct path s_{LOS} (blue) and 25 independent received s_R multipath signals (gray) in (4.1).



(b) Probability Mass Function for estimated power in 1000 independent received s_R multipath signals.

Figure 4.28: Characterization of Rayleigh faded multipath channel created using `Matlab`® 's *rayleighchan.m* function.

Table 4.1: Model Development (M) and RF-DNA Fingerprint Testing (T) Conditions for (M#,T#) Multipath Scenarios.

Variable	Description
M1	Models developed using RF-DNA fingerprints extracted from signal responses with **No Multipath Present**.
M2	Models developed using RF-DNA fingerprints extracted from signal responses with **Multipath Present**.
T1	*Classification* is performed using RF-DNA testing fingerprints extracted from signal responses with **No Multipath Present**.
T2	*Classification* is performed using RF-DNA testing fingerprints extracted from signal responses with **Multipath Present**.

3. Both model development and *classification* performed using RF-DNA extracted from signal responses with ***multipath present***, (M2, T2),

where the combinations of model development and *classification* used for multipath assessment are denoted herein as (M#,T#) with # taking on values indicated in the variable column of Table 4.1.

For this initial investigation RF-DNA fingerprint generation, model development, and subsequent *classification* were performed using direct path signals with scaled background noise $n_b[k]$ added to achieve SNR=[9.0, 15.0, 18.0] dB; resultant MDA/ML *classification* performance for each of these SNR conditions are shown in Fig. 4.29 (18.0 dB), Fig. 4.30 (15.0 dB), and Fig. 4.31 (9.0 dB). Notable observations from these results include:

1. Figure 4.29 presents results for SNR=18.0 dB and reflects an approximate 50% reduction in average GT−based *classification* performance when comparing the (M1,T1) and (M1,T2) scenarios. When comparing scenario one (M1, T1) and two (M1, T2), there is an approximate 15% and 35% reduction in average *classi-*

fication performance when using RF-DNA fingerprints generated from GT and GWT-based features, respectively. For the (M2,T2) scenario using GWT-based RF-DNA, average performance degrades by approximately 15% when compared with the (M1,T1) scenario. However, the average results of scenario three are consistent between the GT and GWT-based RF-DNA fingerprints. For scenario two (M1,T2), GWT-based RF-DNA results in an approximate improvement of 15% in average *classification* performance in comparison to the results when using GT-based RF-DNA. This suggests that GWT-based RF-DNA fingerprints provide some multipath resilience.

2. The resiliency of GWT-based RF-DNA fingerprints to multipath is tested by repeating the above process for SNR=[9.0, 15.0] dB. The SNR=15.0 dB *classification* performance results are shown in Fig. 4.30 using both GT and GWT features under the three (M#,T#) scenarios detailed above. Comparison of (M1,T1) and (M1,T2) scenario results shows that average *classification* performance is degraded by approximately 45% and 32% for GT and GWT-based RF-DNA, respectively. For the (M2,T2) scenario, average percent *classification* is consistent across both fingerprint types. As with SNR=18.0 dB results in Fig. 4.29, GWT-based fingerprinting at SNR=15.0 dB provides an improvement of 15% when compared with GT-based *classification* results for the (M1,T2) scenario and demonstrates the resiliency of GWT RF-DNA under multipath conditions.

3. Figure 4.31 shows results for SNR=9.0 dB. As with the previous two investigated SNRs, test scenario two (M1,T2) results in a degradation of performance versus that of scenario one (M1,T1) for both fingerprint generation techniques. However, the scenario two GWT-based average *classification* performance results in only a marginal improvement (approximately 2%) over that of the GT-based results. Test scenario three remains consistent between the GT and GWT-based RF-DNA average *classification* results and provides marginal improvement over the (M1,T2) scenario. These results and those of test scenario

two suggests that the multipath resiliency benefits of the non-linear GWT are minimized/lost as SNR degrades.

4. When comparing the results presented in Fig. 4.29, Fig. 4.30, and Fig. 4.31, it is apparent that as SNR degrades the benefits of non-linear GWT-based features, with respect to *classification* performance, are diminished. This is not only the case when comparing GT-based results to those of the GWT, but also when comparing scenario one to two across and within T-F RF-DNA fingerprint generation techniques. Lastly, training and *classification* performed on RF-DNA fingerprints, generated from signals, in which multipath is present proves beneficial to classifier performance when compared to training the classifier using RF-DNA fingerprints without the presence of multipath.

Observation: Use of non-linear GWT features is generally more robust at higher SNR but yields comparable performance to linear GT features when used at lower SNR.

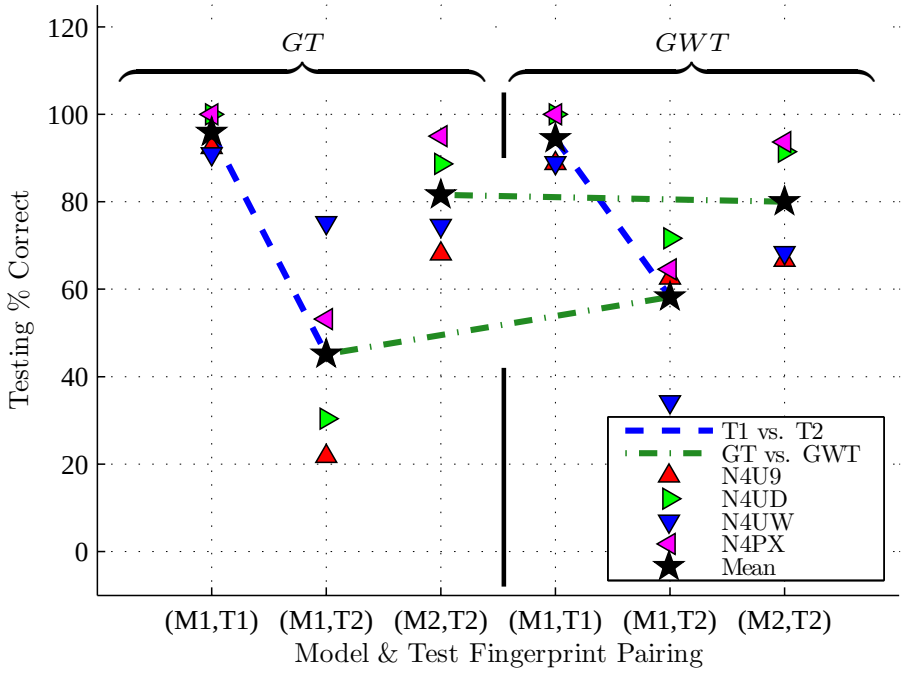


Figure 4.29: MDA/ML multipath assessment using GT (linear) and GWT (non-linear) 802.11 WiFi features with and without multipath present at SNR=18.0 dB.

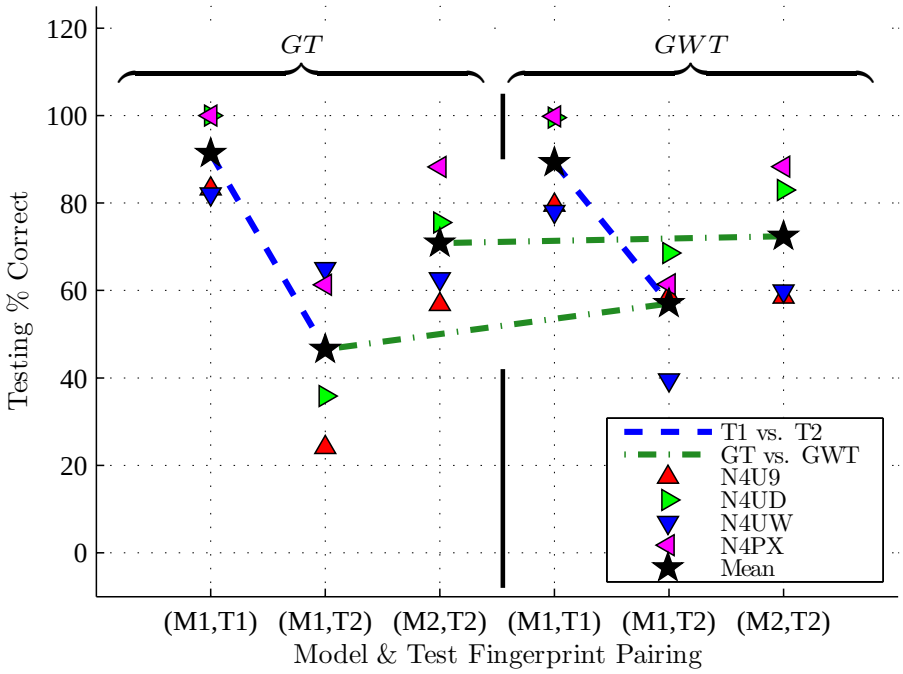


Figure 4.30: MDA/ML multipath assessment using GT (linear) and GWT (non-linear) 802.11 WiFi features with and without multipath present at SNR=15.0 dB.

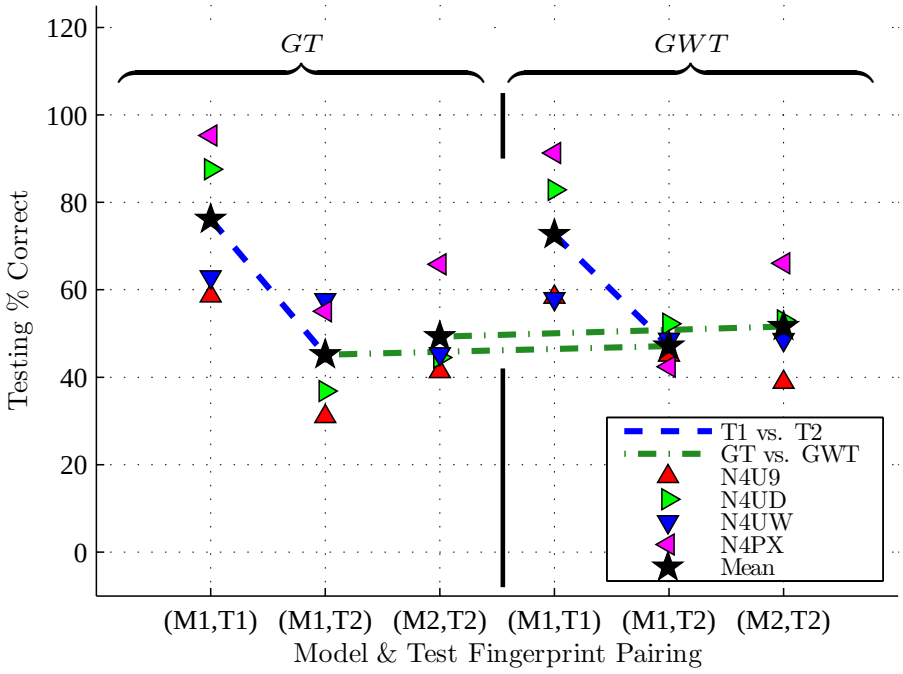


Figure 4.31: MDA/ML multipath assessment using GT (linear) and GWT (non-linear) 802.11 WiFi features with and without multipath present at SNR=9.0 dB.

V. Conclusions

THIS chapter provides a comprehensive summary of key research activities, findings, and recommendations for future research.

5.1 Research Summary

Opportunistic "hackers" continue to gain unauthorized access to wireless networks and their criminal activities are projected to continue as new technologies emerge [10,11,15]. The pervasiveness of communication standards based on Orthogonal Frequency Division Multiplexing (OFDM), e.g., IEEE 802.11a/g Wireless Fidelity (WiFi), IEEE 802.16e Worldwide Interoperability for Microwave Access (WiMAX), and 3GPP Long Term Evolution (LTE), increases the threat of unauthorized access which remains a concern for OFDM-based wireless networks. This concern becomes even greater when considering that some of these technologies are being deployed to form critical links in larger system architectures such as Smart Grid, Supervisory Control And Data Acquisition (SCADA), next generation airport communications, and as backbone/backhaul elements for cloud computing [28, 32, 37, 61, 91]. Similar to 802.11 WiFi wireless networks, the network architectures of WiMAX and LTE are functionally dependent upon Wireless Access Points (WAP) which have been identified as one of the top 10 IT security threats [2]–the motivation for this research addressing WAP security enhancement using RF air monitoring with RF "Distinct Native Attribute" DNA (RF-DNA) fingerprinting.

The seven layer Open Systems Interconnection (OSI) model characterizes and standardizes all services implemented within a wireless network. Conventional mechanisms for network security and detection of unauthorized users have been employed within higher layers of the OSI model, to include the Network (NWK) and Data Link Layer (DLL). Previous research in [17, 60, 65, 78, 85, 96] focused on developing bit-level security mechanisms for detecting and mitigating unauthorized network access. Thus, by design these bit-level techniques overlook inherent Physical (PHY) layer information that is available at WAP "doorways" through which a majority

of criminal activity occurs. Indifference to PHY layer information neglects potentially discriminating information that is contained within *all* wireless network RF emissions, regardless if such emissions are from *authorized* or *unauthorized* devices–reliable discrimination of friend-or-foe devices enhances network security by reliable granting access to authorized users while detecting and countering spoofing attacks of unauthorized users.

RF fingerprinting is one PHY layer technique that leverages inherent discriminating information within wireless RF emissions. This is accomplished by exploiting features that are unique and difficult to counterfeit, i.e., features that are inadvertently imparted onto the RF waveform by the hardware components that constitute the wireless device. A substantial amount of research has been conducted in the area of RF fingerprinting over the past two decades [23–25, 27, 29, 31, 33, 36, 38–41, 44, 47, 49, 54, 56–58, 67, 71, 74–76, 81, 84, 86, 88, 89, 93–95]. Recent related work in [44, 45, 47, 56–58, 71–73, 76, 81, 93, 94] focused on PHY layer exploitation using RF-DNA extracted from selected portions of intentionally modulated signal responses. The RF-DNA attributes are 1) adequately "distinct" to enable persistent cross-device discrimination, and 2) "native" in that the hardware implementation, component type, manufacturing processes and/or environmental interaction variations induce unique unintentional "coloration" on the intentional modulation features–inherent RF-DNA features are sufficiently unique to enable human-like device hardware discrimination.

While a considerable amount of RF-DNA fingerprinting research had been conducted previously, there remained a need at the onset of this research to improve the experimental-to-operational transition potential of RF-DNA fingerprinting and facilitate successful fielding of a system to provide reliable and robust PHY layer security augmentation. Such a security system must be able to discriminate between 1) devices from different manufacturers (cross-manufacturer), 2) dissimilar model devices from the same manufacturer (cross-model), and 3) like model devices from the same manufacturer (the most challenging serial number discrimination case [44, 47, 57, 76, 93, 94]).

The security system must also be able to resolve a given device's bit-level credentials (MAC address, IMEI number, SIM Number, and/or ESN) and RF-DNA fingerprints with the stored reference model associated with the claimed bit-level credentials. This device ID *verification* must be performed in a reliable, timely manner for *authorized* devices while at the same time detecting the presence of *unauthorized* rogue devices attempting to illegitimately gain network access.

5.2 Research Contribution Areas

As summarized below, several important research contributions were made to RF-DNA fingerprinting that enhance its experimental-to-operational transition potential. These contributions include:

5.2.1 2D Gabor-Based RF-DNA. One approach for improving device *classification* performance is the discovery of a more powerful feature set using a given classifier, where increased power is indicated by either 1) requiring a lower SNR to achieve a given *classification* level, or 2) achieving a higher *classification* level for a given SNR. The 802.11a WiFi work by Klein in [56–58] was AFIT's first successful transition from 1D Time/Spectral Domain (TD/SD) feature sets to a 2D joint Time-Frequency (T-F) feature set derived from Dual-Tree $\mathbb{C}$omplex Wavelet Transform (DT-$\mathbb{C}$WT) coefficients. Klein's results for an MDA/ML classifier showed that 2D DT-$\mathbb{C}$WT features were indeed superior with a relative performance "gain" (reduction in required SNR to achieve a given *classification* accuracy) of $G_p \approx$6.0 dB (TD) and $G_p \approx$-3.0 dB (SD) realized for an arbitrary $\%C \geq 90\%$ performance benchmark [56–58, 94].

Gabor Transform (GT) and Gabor-Wigner Transform (GWT) features are introduced here as 2D alternatives to the DT-$\mathbb{C}$WT. Performance was assessed here for both MDA/ML and GRLVQI classifiers using GT/GWT RF-DNA feature sets. For the same 802.11a WiFi devices used by Klein in [56–58], average MDA/ML *classification* performance using full-dimensional (N_f=363 features) GT-based RF-DNA

fingerprints achieved the $\%C \geq 90\%$ benchmark for $SNR \geq 9.0$ dB. This corresponds to performance gains of $G_p \approx [9.5,\ 16.6,\ 9.1,\ 7.1]$ dB for GWT, TD, SD, and DT-$\mathbb{C}$WT-based RF-DNA fingerprinting, respectively–RF-DNA fingerprints derived from 2D GT-based features are indeed superior to previous 1D and 2D feature sets [71–73, 76].

Results for 802.16e WiMAX Mobile Subscriber (MS) devices were equally significant, with MDA/ML classifier performance using full dimensional (N_f=204 features) GT-based RF-DNA fingerprints reaching the arbitrary $\%C \geq 90\%$ benchmark for $SNR \geq 6.5$ dB and achieving performance gains of $G_p \approx [4.9,\ 8.1,\ 20.0]$ relative to GWT, TD, and SD RF-DNA fingerprints, respectively [71, 76]. Corresponding GRLVQI classifier results using the same input feature set were marginally poorer, with the arbitrary $\%C \geq 90\%$ benchmark reached at $SNR \geq 10.0$ dB and appreciable gains of $G_p \approx [6.5,\ 12.5]$ dB achieved for GWT and TD RF-DNA fingerprints, respectively [45, 72, 73]. Related research using other signal types suggests that SNR=10.0 dB is achievable in operational environments such that implementation of GRLVQI processing is feasible. Of equal importance, the inherent feature relevance indication provided by GRLVQI overcomes a major MDA/ML limitation and enables efficient processing using dimensionally reduced feature sets–the next highlighted research contribution.

5.2.2 Dimensional Reduction Analysis (DRA). Although the MDA/ML classifier performed favorably in previous works and for generating baseline results under this research, it has one major limitation that impacts its potential for experimental-to-operational transition–it lacks a mechanism for relating input feature impact to the final *classification* decision. This limitation inhibits the ability to retain or discard a given feature, based upon its relevance to *classification*, for future feature generation and subsequent *classification*. The ability to select and retain a most relevant set of RF-DNA features, while maintaining a given *classification* accuracy, is assessed here using Dimensional Reduction Analysis (DRA). The dimensionally reduced feature set requires fewer computational resources (processing power, memory, etc.) which

increases the experimental-to-operational transition potential. The MDA/ML limitation is overcome here using GRLVQI which inherently develops a feature relevance ranking for each RF-DNA input feature during classifier training.

Given GRLVQI relevance rankings, the effectiveness of four DRA feature selection methods were investigated under this research, including [45, 72, 73]:

i. **DRA Method #1**: Use the highest ranked relevance values produced at a single SNR to evaluate *classification* performance at all SNR per equation (3.17).

ii. **DRA Method #2**: Use the highest ranked relevance values for each investigated SNR to assess *classification* performance at the same SNR per equation (3.18).

iii. **DRA Method #3**: Use the highest ranked relevance values based on the average relevance rankings computed across all investigated SNR per equation (3.19).

iv. **DRA Method #4**: Use the union of highest ranked relevance values across all SNR considered per equation (3.20).

Results in Section 4.1.3 and Section 4.2.3 show that for DRA≈90% (90% of full-dimensional RF-DNA input features discarded), statistically equivalent *classification* performance is achieved for a 10× reduction in computation time [45, 72, 73]. Of the four methods considered, DRA Method #3 resulted in the best overall *classification* performance for all feature sets (TD, SD, GT, and GWT) and range of SNR considered. A key advantage of DRA Method #3 is that it provides a means for determining a single, SNR independent set of features that can be applied without requiring real-time burst SNR estimates in operational network security systems. *Classification* results using DRA feature sets with each of the classifiers include:

1. For 802.16e WiMAX devices with dimensionally reduced feature sets (N_f=20 of 204 total features) selected using DRA Method #3: 1) the MDA/ML classifier achieved individual device *classification* accuracies of $\%C \geq 80\%$ for five of the six devices at $SNR \geq 9.0$ dB, and 2) the GRVLQI classifier achieved $\%C \geq 80\%$ for all six devices at $SNR \geq 15.0$ dB.

2. For 802.11a WiFi devices with dimensionally reduced feature sets (N_f=36 of 363 total features) selected using DRA Method #3: 1) the MDA/ML classifier achieved the arbitrary $\%C \geq 90\%$ benchmark at $SNR \geq 12.0$ dB, and 2) the GRVLQI classifier achieved the arbitrary $\%C \geq 90\%$ benchmark is achieved for $SNR \geq 16.0$ dB.

5.2.3 Device ID Verification. A majority of prior related RF-DNA fingerprinting work predominantly focused on device *classification* (a one-to-many looks "most like" assessment) [44, 47, 57, 74–76, 81, 93, 94]. In this case, the network security system uses a similarity measure to compare an *unknown* device's "challenge" RF-DNA fingerprint to stored reference models associated with each of the N_C^A *known/-authorized* network devices. The security system then declares the *unknown* device as being one the specific *authorized* devices based on the reference model providing the "best" match to the current "challenge" fingerprint(s). This declaration is made regardless of whether or not the "challenge" fingerprints originate from an *authorized* or *unauthorized* device. This "best" match assignment may actually be a poor match and creates the opportunity for "rogue" devices, whose RF-DNA closely resembles that of an *authorized* device, to gain access to the *unauthorized* network access. Furthermore, the one-to-many device *classification* approach may not be feasible in applications where the network is comprised of a large number of devices or a network in which users enter and leave frequently or randomly.

This research adopted the MDA/ML-based *verification* methods used for unintentional emissions in [19, 20] and expanded their applicability to include: 1) intentional wireless emissions, and 2) implementation with a GRLVQI classifier [71–73]. As designated in [19, 20] and maintained here, device ID *verification* (a one-to-one looks "how much" like assessment) involves a comparison between an *unknown* device's "challenge" fingerprint(s) and a stored reference model affiliated with the *claimed* bit-level identity being presented by the device. This comparison is made using similarity measures (*verification* test statistics) that are based on Bayesian posterior

probabilities and geometric measures. The geometric measures considered under this research included Euclidean Distance, Normalized Euclidean Distance, Spatial Angle, and the product of Spatial Angle and Normalized Euclidean Distance.

Device ID *verification* performance using 802.16e WiMAX devices with MDA/ML-based Bayesian posterior probabilities included achieving an arbitrary Equal Error Rate (EER) of EER$\leq$10% benchmark for *all* six authorized devices at SNR=6.0 dB. For GRLVQI-based geometric measures, the product of Spatial Angle and Normalized Euclidean Distance proved superior with *all* six authorized WiMAX devices achieving the arbitrary EER$\leq$10% benchmark at SNR=18.0 dB. To simulate a network spoofing attack, GRLVQI-based *verification* was performed using six *unauthorized* "rogue" WiMAX devices presenting false bit-level credentials matching each of the *authorized* device–a total of 36 independent network intrusion attacks via spoofed bit-level identities. Using the GRLVQI-based Spatial Angle times Normalized Euclidean Distance similarity measure, 35 of 36 attacks were successfully detected, with EER$\leq$10% (Rogue Rejection Rate RRR$\geq$90%) at SNR=18.0 dB [72].

For completeness, Device ID *verification* performance was assessed using the four available 802.11a WiFi devices. This was done using the GRLVQI-based Spatial Angle times Normalized Euclidean Distance similarity measure. In this case, the arbitrary EER$\leq$10% benchmark was achieved for *all* four *authorized* 802.11a WiFi devices at SNR=15.0 dB. Given the limited number of 802.11a devices, rogue rejection was not assessed and remains an area of interest for future research.

5.3 Recommendations for Future Research

As outlined in Section 1.2, the decision to investigate Gabor-based RF-DNA fingerprinting and GRLVQI *classification* was motivated by two factors, including 1) improving device *classification* performance relative to previous RF fingerprinting work [23–25, 27, 29, 31, 33, 36, 38–41, 44, 47, 49, 54, 56–58, 67, 74, 75, 81, 84, 86, 88, 89, 93–95] and 2) addressing noted shortcomings of the MDA/ML classifier. Relative to

previous RF fingerprinting work, the utilization and benefits of Gabor-based features and GRLVQI *classification* has been acutely demonstrated and well-received within the technical community [71–73, 76]. However, there remains several related topics of interest that warrant further investigation, including:

1. **Alternate Wireless Devices**: Demonstration results presented here are based on experimentally collected IEEE 802.11a WiFi signals from Cisco AIR-CB21G-A-K9 cards and IEEE 802.16e WiMAX signals from Alvarion BreezeMAX Extreme 5000 WiMAX MS units. There are many other manufacturers of WiFi and WiMAX subscriber equipment. Additional research could be conducted to apply techniques developed in this work using emissions from other WiFi (NetGear, Linksys, Etc.) and WiMAX (Motorola, Alcatel, Etc.) user equipment. Also, Fourth Generation (4G) Long Term Evolution (LTE) is an OFDM-based wireless standard that is being deployed throughout the world to replace older Third Generation (3G) Global System for Mobile Communications (GSM) standard. The application of Gabor-based RF-DNA fingerprinting with GRLVQI *classification* and *verification* could be considered for securing LTE and other 4G network architectures employing WAPs.
2. **Alternate Classifiers**: This work introduced the ANN-based GRLVQI classifier to address shortcomings of earlier work using a Fisher-based MDA/ML classifier. One of the key GRLVQI advantages exploited under this research, and which is not supported by MDA/ML, is the capability to determine which input features are most relevant to overall *classification* performance. The GRLVQI classifier implemented here uses a weighted Euclidean distance as the *classification* similarity measure. While effective, it is believe that other similarity measures (e.g., $l1$-norm, spatial angle, spatial angle times distance, etc.) may improve upon GRLVQI *classification* performance. This suggestion is based on the effectiveness of alternate measures that were used here for demonstrating reliable device ID *verification*. Additional research at AFIT suggests that the Learning From Signals (LFS) classifier may be effective as well given that it per-

forms consistently with MDA/ML while providing a feature relevance indication similar to GRLVQI [14, 44–47].

3. **Alternate Channel Models**: The disparity between collected SNR_c and analysis signal SNR_A was such that the like-filtered Additive White Gaussian Noise (AWGN) dominated the collected background noise. Thus, the the research results are most consistent with what is expected for AWGN channel conditions. The signal collection environment and methodology could be modified such that actual SNR_c variation is induced and analysis signal generation removed. Additionally, only the impact of a single multipath reflector was considered to provide a preliminary assessment of performance using linear (GT) and nonlinear (GWT) features. The GWT feature set provided only modest additional robustness to simple multipath and more complex multipath models (e.g., typical urban, rural, etc.) should be considered to sufficiently address technical community "encouragement" and provide much needed demonstration results.
4. **Network/Cross-Layer Integration**: This work has demonstrated the applicability of RF-DNA fingerprinting for supporting one-to-one device ID *verification* as well as one-to-many device *classification*. Specifically, the PHY-based methods herein support envisioned bit-level security augmentation using RF air monitoring under network (NWK) control at WAPs. The effectiveness of an integrated PHY-NWK cross-layer framework remains to be demonstrated and could be pursued. This cross-layer coordination could be used to provide one-to-one Multi-Factor *Verification* of authorized network devices.

5.4 Sponsor Acknowledgment

Research sponsored in part by the U.S. Air Force Research Laboratory, Sensors Directorate (AFRL/RY), Wright-Patterson Air Force Base, OH. Results here directly support AFRL/RY's mission which aims to "ensure unequaled reconnaissance, surveillance, precision engagement, and electronic warfare capabilities for America's Air and

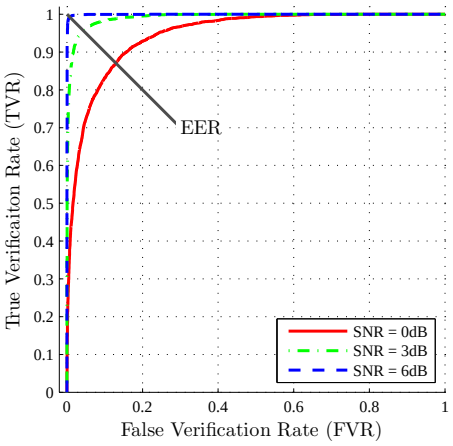
Space Forces by developing, demonstrating and transitioning advanced sensors and sensor technologies." [90].

Appendix A. Additional Results

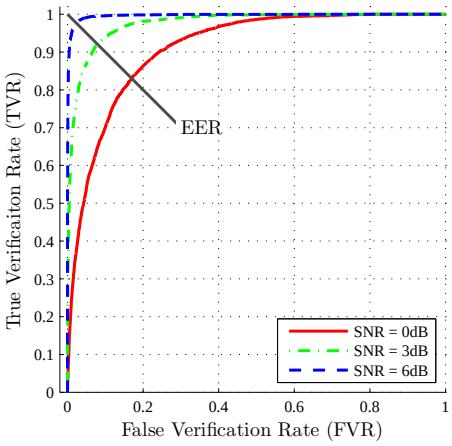
THIS appendix contains the additional results not presented in Chapter IV. These additional results are presented here in the same order as presented in the document above.

A.1 WiMAX Device ID Verification

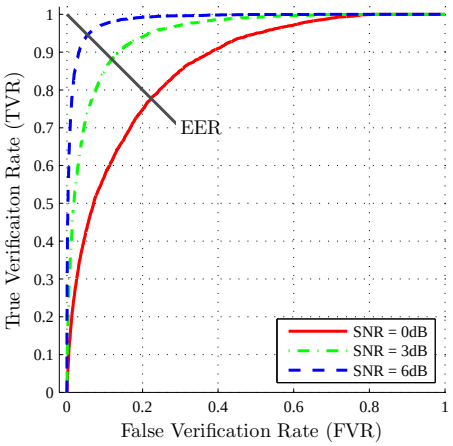
Here are the device *verification* results for the remaining four *Authorized* and five *Rogue* WiMAX MS devices.



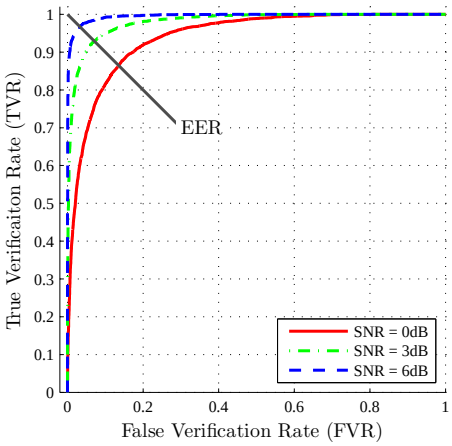
(a) MS63A7.



(b) MS63A9.



(c) MS6373.



(d) MS6387.

Figure A.1: ROC curves and EER for four WiMAX MS devices at SNR=[0, 3, 6] dB using an a posterior probability *verification* test statistic z_v.

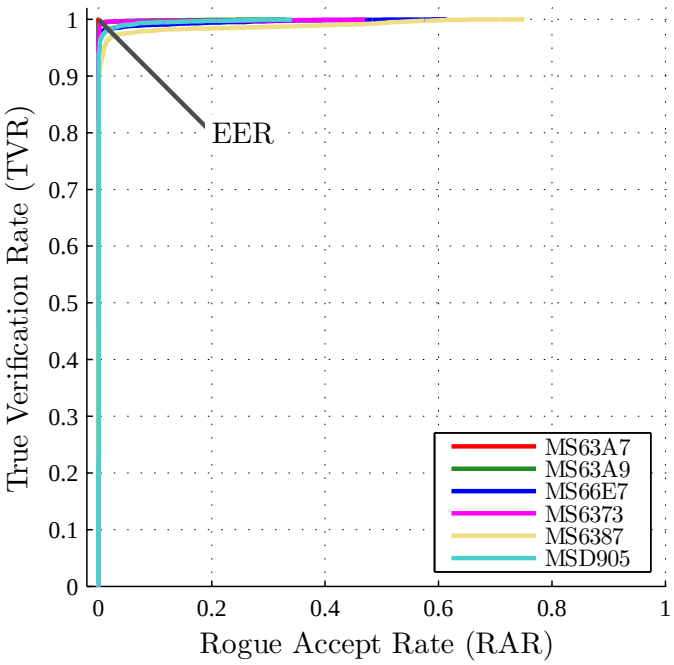


Figure A.2: ROC curves and EER for *Rogue* WiMAX MS device MS9993 at SNR=18 dB using a Euclidean Distance *verification* test statistic z_v

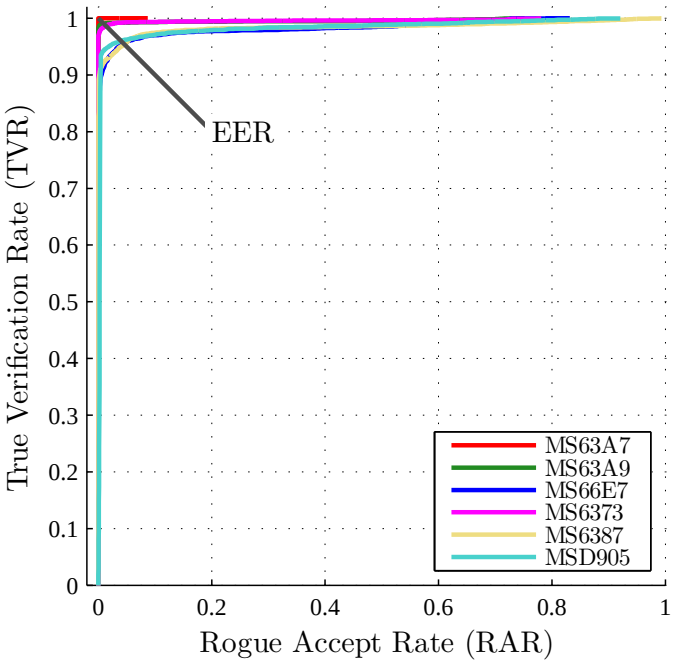


Figure A.3: ROC curves and EER for *Rogue* WiMAX MS device MSC2FF at SNR=18 dB using a Euclidean Distance *verification* test statistic z_v.

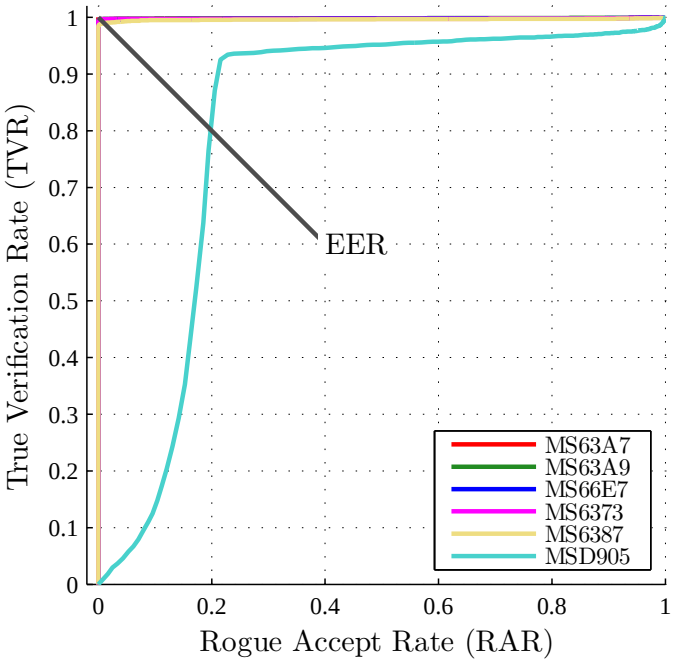


Figure A.4: ROC curves and EER for *Rogue* WiMAX MS device MSDAB9 at SNR=18 dB using a Euclidean Distance *verification* test statistic z_v.

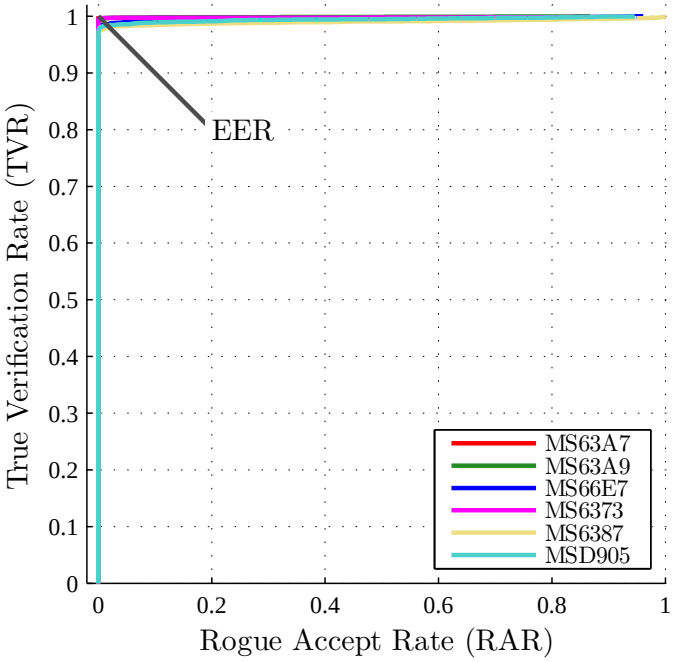


Figure A.5: ROC curves and EER for *Rogue* WiMAX MS device MSDAC5 at SNR=18 dB using a Euclidean Distance *verification* test statistic z_v.

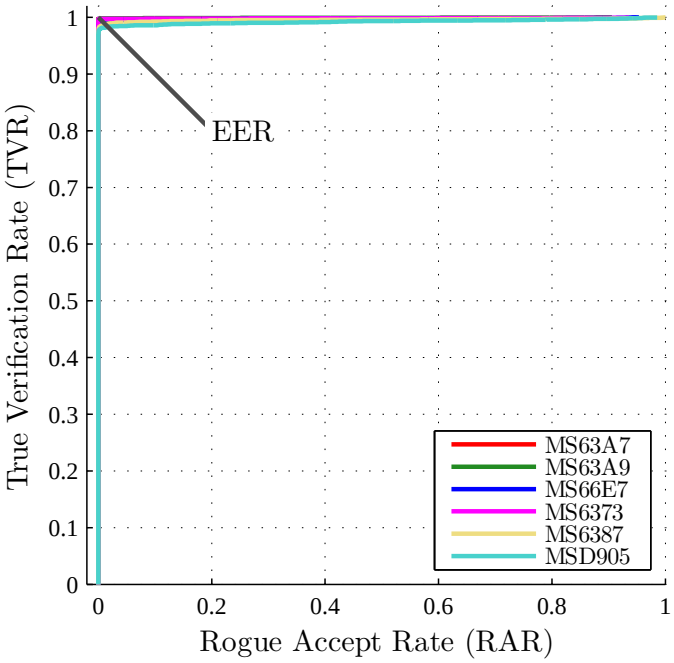


Figure A.6: ROC curves and EER for *Rogue* WiMAX MS device MSDDBF at SNR=18 dB using a Euclidean Distance *verification* test statistic z_v.

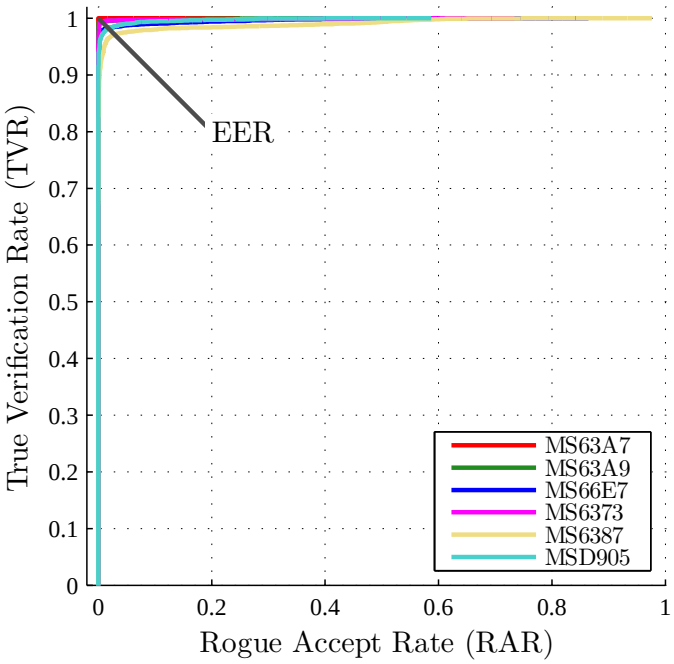


Figure A.7: ROC curves and EER for *Rogue* WiMAX MS device MS9993 at SNR=18 dB using a Normalized Euclidean Distance *verification* test statistic z_v.

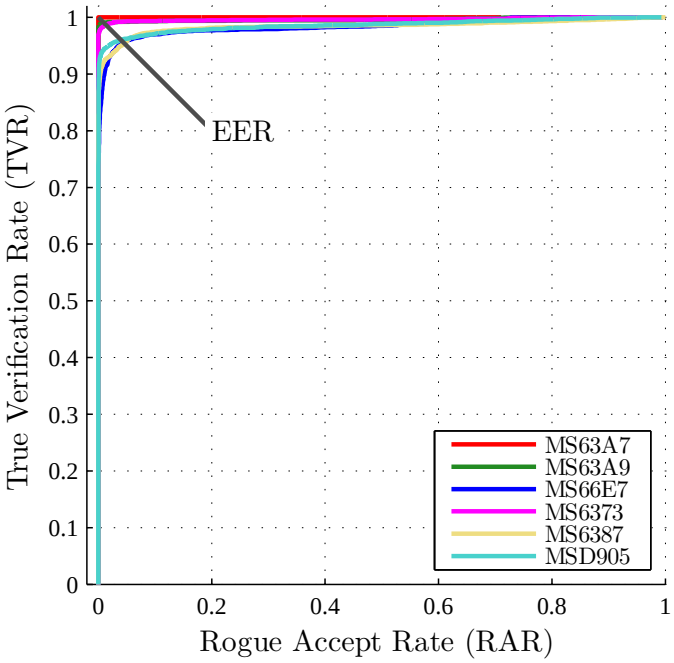


Figure A.8: ROC curves and EER for *Rogue* WiMAX MS device MSC2FF at SNR=18 dB using a Normalized Euclidean Distance *verification* test statistic z_v.

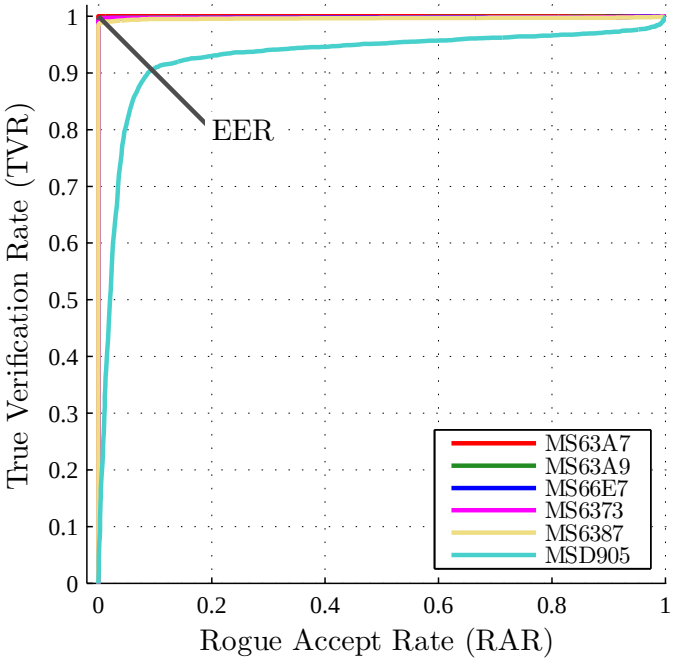


Figure A.9: ROC curves and EER for *Rogue* WiMAX MS device MSDAB9 at SNR=18 dB using a Normalized Euclidean Distance *verification* test statistic z_v.

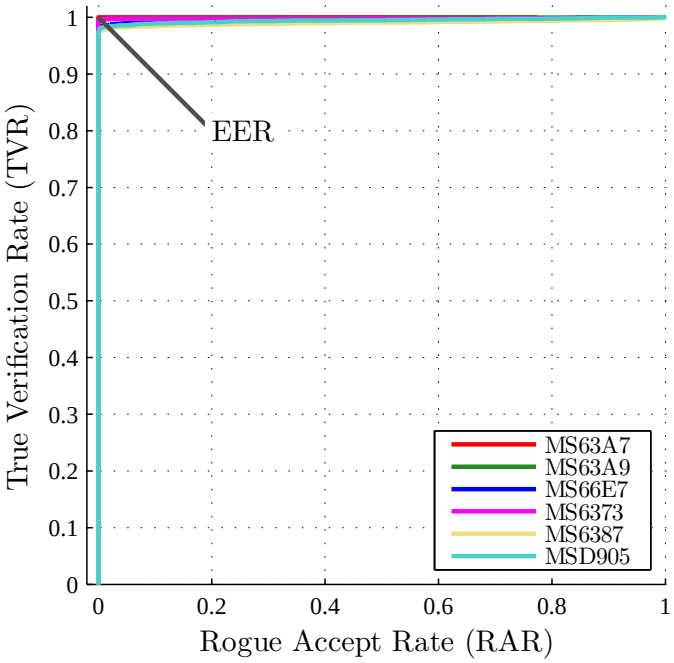


Figure A.10: ROC curves and EER for *Rogue* WiMAX MS device MSDAC5 at SNR=18 dB using a Normalized Euclidean Distance *verification* test statistic z_v.

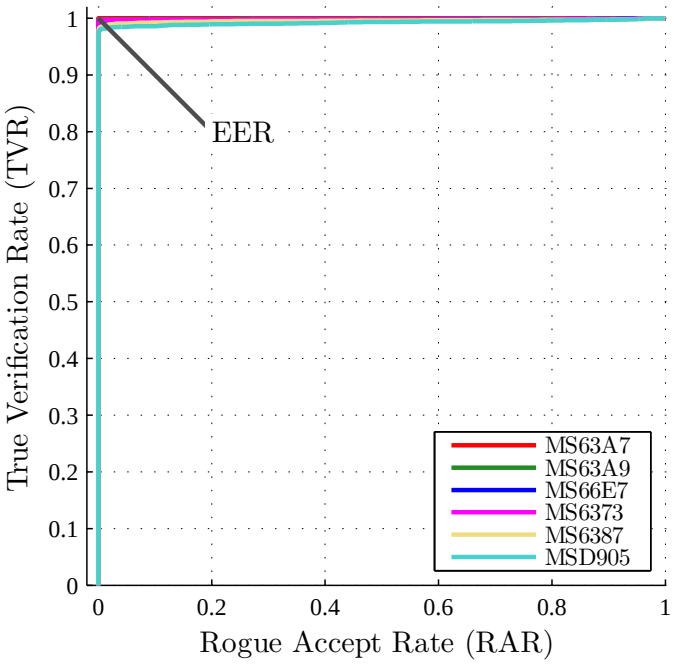


Figure A.11: ROC curves and EER for *Rogue* WiMAX MS device MSDDBF at SNR=18 dB using a Normalized Euclidean Distance *verification* test statistic z_v.

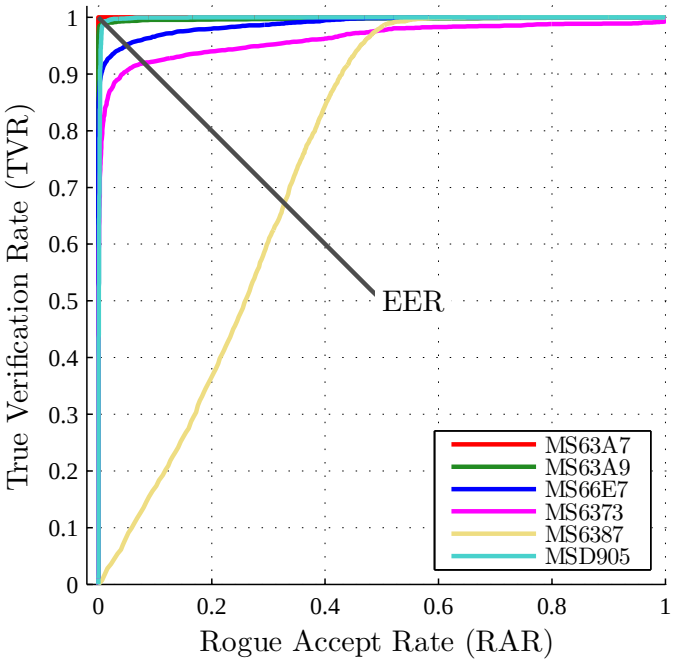


Figure A.12: ROC curves and EER for *Rogue* WiMAX MS device MS9993 at SNR=18 dB using a Spatial Angle *verification* test statistic z_v.

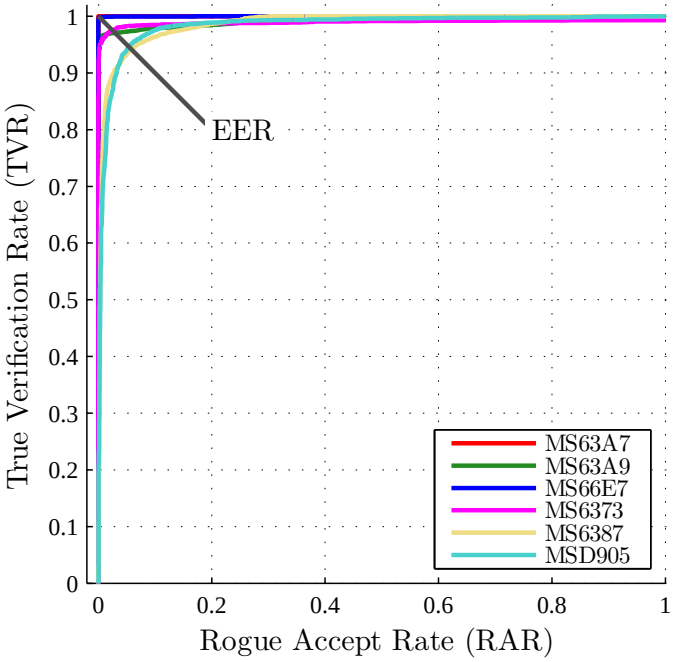


Figure A.13: ROC curves and EER for *Rogue* WiMAX MS device MSC2FF at SNR=18 dB using a Spatial Angle *verification* test statistic z_v.

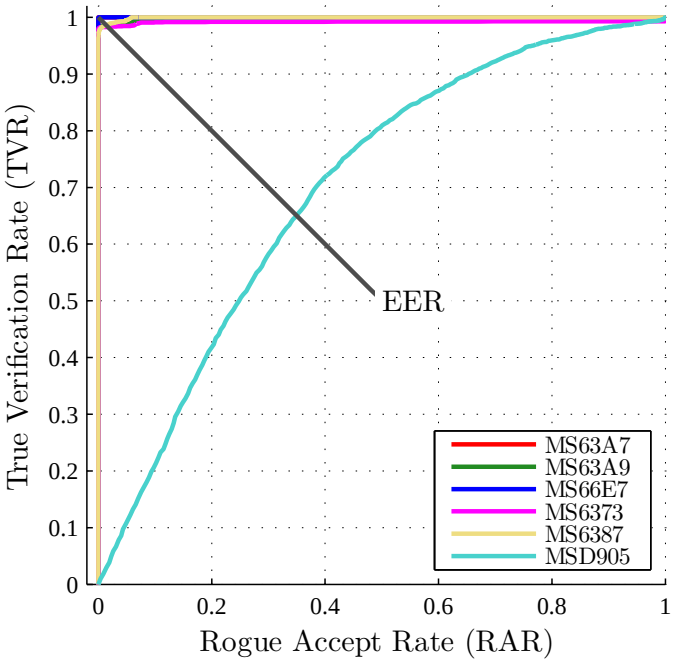


Figure A.14: ROC curves and EER for *Rogue* WiMAX MS device MSDAB9 at SNR=18 dB using a Spatial Angle *verification* test statistic z_v.

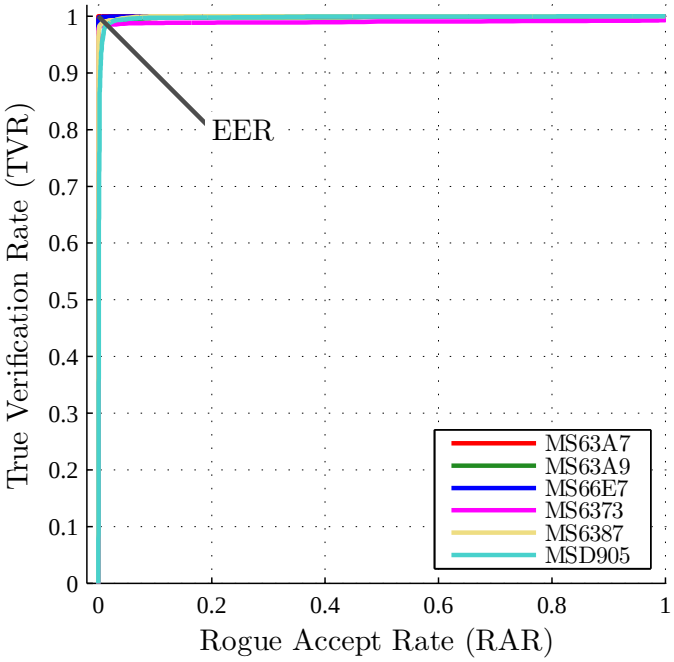


Figure A.15: ROC curves and EER for *Rogue* WiMAX MS device MSDAC5 at SNR=18 dB using a Spatial Angle *verification* test statistic z_v.

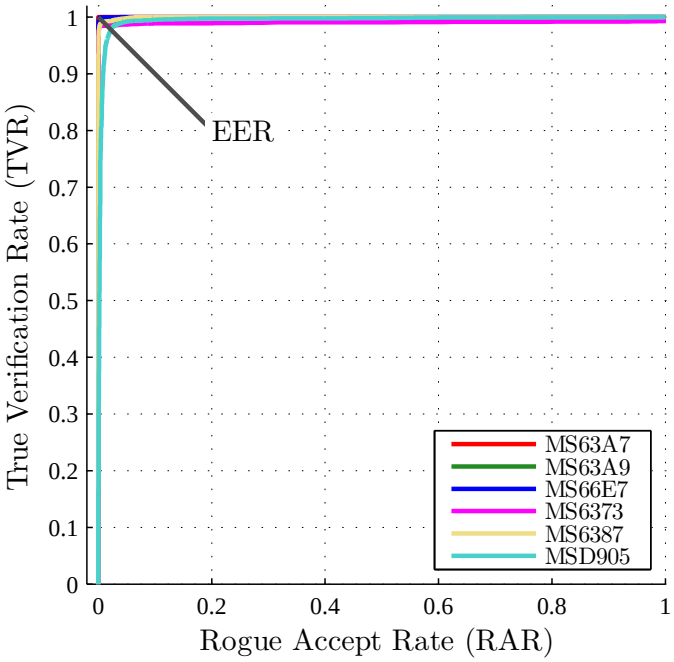


Figure A.16: ROC curves and EER for *Rogue* WiMAX MS device MSDDBF at SNR=18 dB using a Spatial Angle *verification* test statistic z_v.

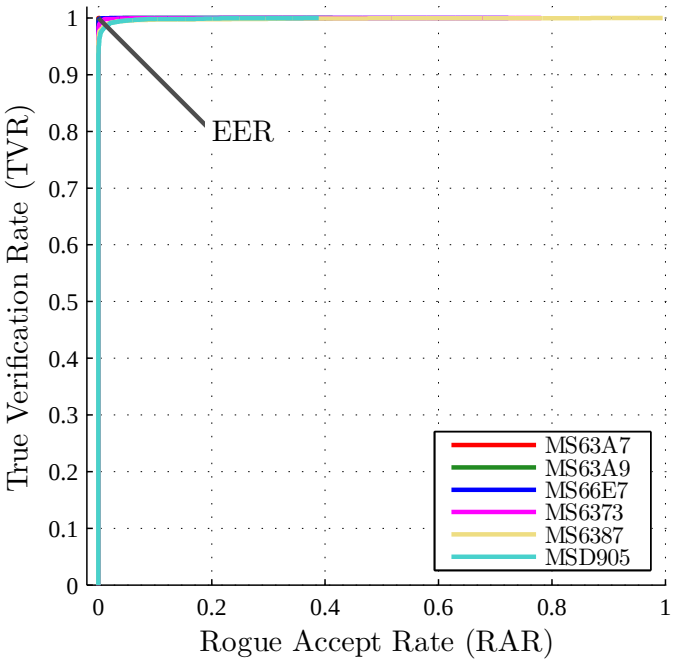


Figure A.17: ROC curves and EER for *Rogue* WiMAX MS device MS9993 at SNR=18 dB using the a Spatial Angle-times-Normalized Euclidean Distance *verification* test statistic z_v.

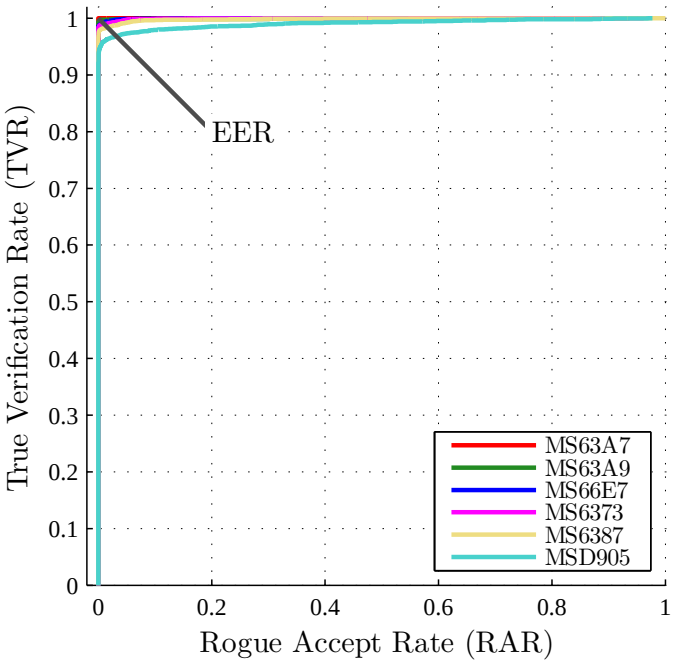


Figure A.18: ROC curves and EER for *Rogue* WiMAX MS device MSC2FF at SNR=18 dB using a Spatial Angle-times-Normalized Euclidean Distance *verification* test statistic z_v.

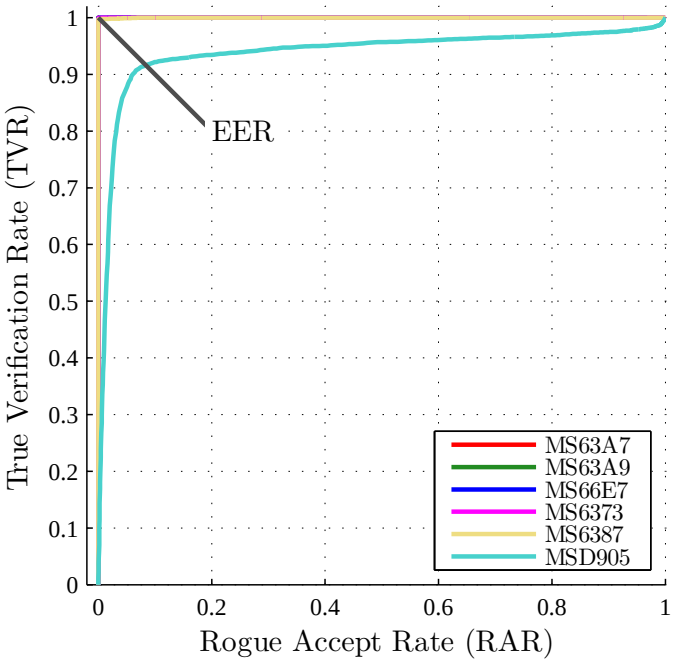


Figure A.19: ROC curves and EER for *Rogue* WiMAX MS device MSDAB9 at SNR=18 dB using a Spatial Angle-times-Normalized Euclidean Distance *verification* test statistic z_v.

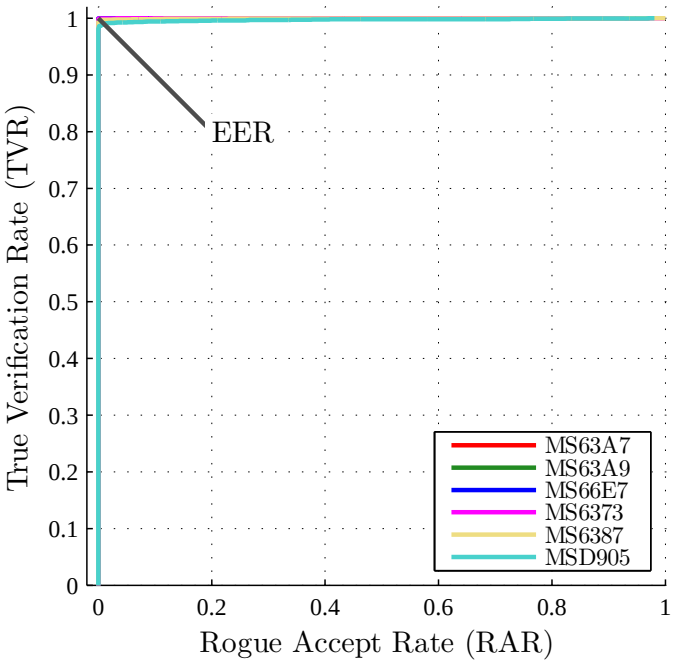


Figure A.20: ROC curves and EER for *Rogue* WiMAX MS device MSDAC5 at SNR=18 dB using a Spatial Angle-times-Normalized Euclidean Distance *verification* test statistic z_v.

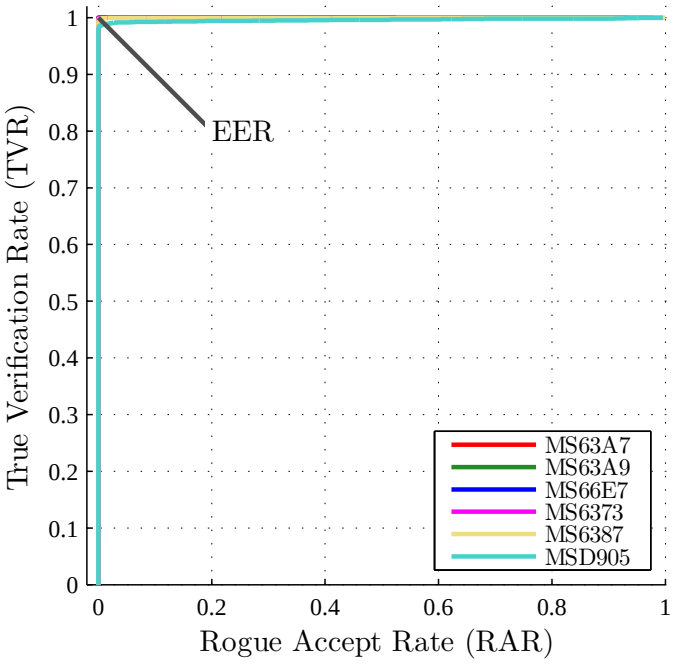
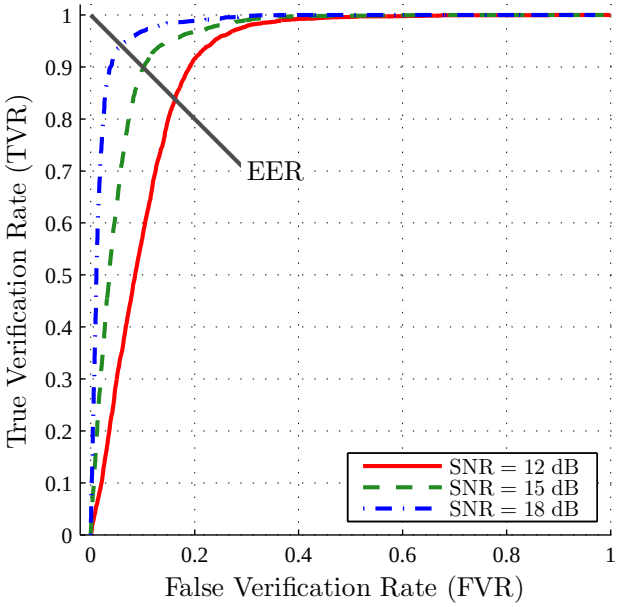


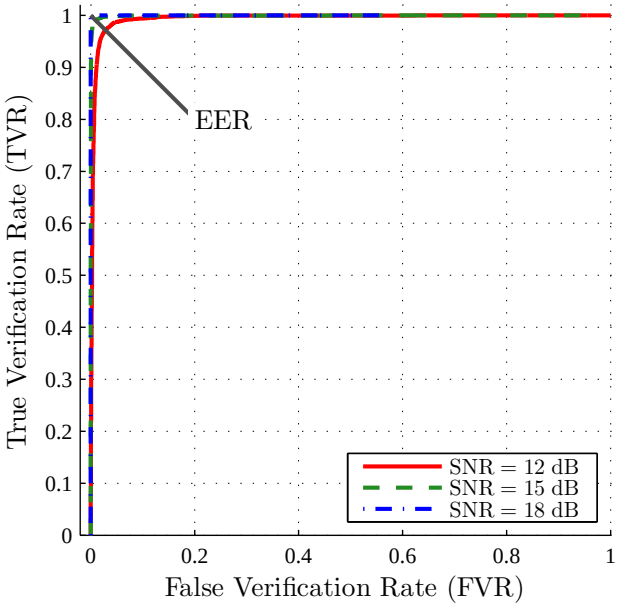
Figure A.21: ROC curves and EER for *Rogue* WiMAX MS device MSDDBF at SNR=18 dB using a Spatial Angle-times-Normalized Euclidean Distance *verification* test statistic z_v.

A.2 WiFi Device ID Verification

Here are the device *verification* results for WiFi devices, N4UW and N4PX, not shown in Section 4.2.4.



(a) WiFi device: N4UW.



(b) WiFi device: N4PX.

Figure A.22: ROC curves and EER for N4UW and N4PX WiFi devices at SNR_A=[12, 15, 18] dB.

Bibliography

1. "OSI Reference Model", Cisco Certified Network Associate (CCNA) Guru Website, www.ccnaguru.com/osi-reference-model.html, May 2009.

2. "Top 10 Network Security Threats", *Government Technology*, www.govtech.com/security/Top-10-Network-Security-Threats.html, Sep 2010.

3. *Internetworking Technology Handbook*. Cisco Systems, Inc., Dec 2009.

4. 3GPP TS 36.201 Ver 10.0.0. *3rd Generation Partnership Project; Technical Specification Group Radio Access Network; Evolved Universal Terrestrial Radio Access (E-UTRA); LTE physical layer; General description (Release 10)*, Dec 2010.

5. 3GPP TS 36.213 Ver 10.2.0 . *3rd Generation Partnership Project; Technical Specification Group Radio Access Network; Evolved Universal Terrestrial Radio Access (E-UTRA); LTE physical layer; Physical layer procedures (Release 10)*, Jun 2011.

6. Agilent Technologies Inc., USA. *Agilent E3238 Signal Intercept and Collection Solutions: Family Overview*, Publication 5989-1274EN, Jul 2004.

7. Alvarion, Edition 215373 Rev. A. *BreezeMAX Extreme 5000: WiMAX 16e Pioneer for the License-Exempt Market*, 2009.

8. Azzouz, E., and A. Nandi. *Automatic Modulation Recognition of Communication Signals*. Kluwer Academic Publishers, Boston, 1996.

9. Bastiaans, M. "Discrete Gabor Transform and Discrete Zak Transform". *1996 IEEE Int'l Conf on Signal and Image Processing Applications (ICSIPA96)*. 1996.

10. Blau, J. "Open-Source Effort to Hack GSM", IEEE Spectrum: Inside Technology, www.spectrum.ieee.org/telecom/wireless/open-source-effort-to-hack-gsm, 2009.

11. Bosworth, S., and M. Kabay (editor). *Computer Security Handbook*. Wiley & Sons, 4^{th} Edition, 2002.

12. Buckner, M. *Learning From Data with Localized Regression and Differential Evolution*. Ph.D. thesis, University of Tennessee, Knoxville, May 2003.

13. Buckner, M., A. Urmanov, A. Gribok, and J. Hines. "Application of Localized Regularization Methods for Nuclear Power Plant Sensor Calibration Monitoring", Technical Correspondence, 2002.

14. Buckner, M., M. Bobrek, E. Farquahar, P. Harmer, and M. Temple. "Enhancing Network Security Using 'Learning-From-Signals' and Fractioinal Fourier Transform Based RF-DNA Fingerprints". *SDR'11- Wireless Innovation Conf*. Dec 2011.

15. Capite, D. *Self-Defending Networks: The Next Generation of Network Security*. Cisco Press, 2006. ISBN 1587052539.

16. Cariolario, G., T. Erseghe, P. Kraniauskas, and N. Laurenti. "A Unified Framework for the Fractional Fourier Transform". *IEEE Trans on Signal Processing*, 46:3206–3212, 1998.

17. Chen, Y., W. Trappe, and R. Martin. "Detecting and Localizing Wireless Spoofing Attacks". 2007 IEEE Conf on Sensor, Mesh and AdHoc Communications and Networks (SECON07), pp. 193-202, Jun 2007.

18. Cho, S., G. Jang, and S. Kwon. "Time-Frequency Analysis for Power-Quality Disturbances via the Gabor-Wigner Transform". *IEEE Trans on Power Delivery*, Vol. 25, No. 1, Jan 2010.

19. Cobb, W. *Exploitation of Unintentional Information Leakage from Integrated Circuits*. Ph.D. thesis, Air Force Institute of Technology, September 2011.

20. Cobb, W., E. Laspe, R. Baldwin, M. Temple, and Y. Kim. "Intrinsic Physical Layer Authentication of ICs". *IEEE Trans on Information Forensics and Security*, 2(4):793–808, Dec 2011.

21. Cohen, L. *Time-Frequency Analysis*. Prentice-Hall, New York, 1995.

22. Corporation, Altera. *Application Note 403: WiMAX OFDMA Ranging, Version 1.0*. Technical report, Washington, August 2006.

23. Danev, B., and S. Kapkun. "Transient-Based Identification of Wireless Sensor Nodes". *8th ACM/IEEE Int'l Conf on Information Processing in Sensor Networks (IPSN09)*. Apr 2009.

24. Danev, B., H. Luecken, S. Capkun, and K. El Defrawy. "Attacks on Physical-layer Identification". *3rd ACM Int'l Conf on Wireless Network Security (WiSec10)*. Mar 2010.

25. Danev, B., T. Heydt-Benjamin, and S. Capkun. "Physical-layer Identification of RFID Devices". *18th Conf on USENIX Security Symposium*, SSYM'09, 199–214. 2009.

26. DeSieno, D. "Adding a Conscience to Competitive Learning". 1998 IEEE Int'l Conf on Neural Networks I, Jul 1988, pp.117-124.

27. Desmond, L., C. Yuan, T. Pheng, and R. Lee. "Identifying Unique Devices Through Wireless Fingerprinting". *1st ACM conference on Wireless Network Security*, WiSec '08, 46–55. ACM, N, 2008.

28. Dikaiakos, M., D. Katsaros, P. Mehra, G. Pallis, and A. Vakali. "Cloud Computing: Distributed Internet Computing for IT and Scientific Research". *Internet Computing, IEEE*, 13(5):10–13, Oct 2009.

29. Dubendorfer, C., B. Ramsey, and M. Temple. "An RF-DNA Verification Process for ZigBee Networks". *2012 Military Communications Conf (MILCOM12)*. Oct 2012.

30. Duda, R., P. Hart, and D. Stork. *Pattern Classification*. John Wiley & Sons, Inc., New York, 2^{nd} Edition, 2001.

31. Ellis, K., and N. Serinken. "Characteristics of Radio Transmitter Fingerprints". *Radio Science*, Vol. 36, No. 4, pp. 585-597, 2001.

32. European Organisation for the Safety of Air Navigation, Edition 1.3, Released Issue. *IEEE 802.16E System Profile Analysis for FCI's Airport Surface Operation*, 30 Sep 2009.

33. Faria, D., and D. Cheriton. "Detecting Identity-Based Attacks In Wireless Networks Using Signalprints". *5th ACM Workshop on Wireless Security*, WiSe '06, 43–52. ACM, New York, NY, USA, 2006.

34. Fawcett, T. *ROC Graphs: Notes and Practical Considerations for Researchers*. Kluwer Academic Publishers, Netherlands, Mar 2004.

35. Gabor, D. "Theory of Communication". *J. Inst. Elect. Eng. (London)*, Vol. 93, No. III, pp. 429-457,1946.

36. Gardner, W. "Signal Interception: A Unifying Theoretical Framework for Feature Detection". *IEEE Trans on Communications*, 36(8):897 –906, Aug. 1988.

37. Hall, E., J. Budinger, R. Diamond, and R. Apaza. "Aeronautical Mobile Communications System Development Status". *Int'l Communications, Navigation and Surveillance Conf (ICNS10)*. May 2010.

38. Hall, J., M. Barbeau, and E. Kranakis. "Detection of Transient in Radio Frequency Fingerprinting Using Signal Phase". IASTED Int'l Conf on Wireless and Optical Communications, May 2003.

39. Hall, J., M. Barbeau, and E. Kranakis. "Radio Frequency Fingerprinting for Intrusion Detection in Wireless Networks", Jul 2005. DRAFT.

40. Hall, J., M. Barbeau, and E. Kranakis. "Detecting Rogue Devices in Bluetooth Networks Using Radio Frequency Fingerprinting". *Communications and Computer Networks*, 108–113. 2006.

41. Hall, J., M. Barveau, and E. Kranakis. "Using Transceiverprints for Anomaly Based Intrusion Detection". 3rd IASTED Int'l Conf on Communications, Internet and Information Technology (CIIT04), Nov 2004.

42. Hall, M. "Correlation-based Feature Selection for Discrete and Numeric Class Machine Learning". 17th Int'l Conf on Machine Learning, 2000.

43. Hammer, B., and T. Villmann. "Generalized Relevance Learning Vector Quantization". *Neural Networks*, 15:1059–1068, 2002.

44. Harmer, P. , M. Williams, and M. Temple. "Using DE-Optimized LFS Processing to Enhance 4G Communication Security". *20th Int'l Conf on Computer Communication and Networks (ICCCN11)*. Aug 2011.

45. Harmer, P., D. Reising, and M. Temple. "Classifier Performance Comparison Using 2D RF-DNA Features". *2013 IEEE Int'l Communications Conf (ICC13)*. Jun 2013, Under Review.

46. Harmer, P., M. Temple, M. Buckner, and E. Farquahar. "4G Security Using Physical Layer RF-DNA with DE-Optimized LFS Classificatioin". *Jour of Communications, Special Issue: Advances in Communications and Networking*, 9(6):671–681, Dec 2011.

47. Harmer, P., M. Temple, M. Buckner, and E. Farquahar. "Using Differential Evolution to Optimize 'Learning from Signals' and Enhance Network Security". *Genetic and Evolutionary Computation Conf (GECCO11)*. Jul 2011.

48. Hastie, T., R. Tibshirani, and J. Friedman. *The Elements of Statistical Learning; Data Mining, Inference, and Prediction*. Springer-Verlag, New York, New York, USA, 2001. ISBN 0-387-95284-5.

49. Hippenstiel, R., and Y. Payal. "Wavelet Based Transmitter Identification". *Signal Processing and Its Applications, 1996. ISSPA 96., Fourth Int'l Symp on*, volume 2, 740–742. Aug 1996.

50. Institute of Electrical and Electronics Engineers, New York, New York, USA. *IEEE Std 802.16e-2005, Local and Metropolitan Area Networks, Part 16: Air Interface for Fixed and Mobile Broadband Wireless Access System*, Feb 2006.

51. Institute of Electrical and Electronics Engineers, New York, NY, 10016-57997, USA. *IEEE Std 802.11-2007, Local and Metropolitan Area Networks, Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications*, Jun 2007.

52. Institute of Electrical and Electronics Engineers, New York, New York, USA. *IEEE Std 802.16-2009, Local and Metropolitan Area Networks, Part 16: Air Interface for Broadband Wireless Access Systems*, May 2009.

53. Jain A., A. Ross, and S. Prabhakar. "An Introduction to Biometric Recognition". *IEEE Trans on Circuits and Systems for Video Technology*, 14(1):4–20, 2004.

54. Jana, S., and S. Kasera. "Wireless Device Identification with Radiometric Signatures". *ACM 14th Int'l Conf on Mobile Computing and Networking (MOBICOM08)*. Sep 2008.

55. Kingsbury, N. "A Dual-Tree Complex Wavelet Transform with Improved Orthogonality and Symmetry Properties". 375–378 vol.2. Sep 2000.

56. Klein, R. *Application of Dual-Tree Complex Wavelet Transforms to Burst Detection and RF Fingerprint Classification*. Ph.D. thesis, Air Force Institute of Technology, September 2009.

57. Klein, R., M. Temple, and M. Mendenhall. "Application of Wavelet-Based RF Fingerprinting to Enhance Wireless Network Security". *Jour of Communications and Networks*, Vol. 11, No. 6, Dec 2009.

58. Klein, R., M. Temple, M. Mendenhall, and D. Reising. "Sensitivity Analysis of Burst Detection and RF Fingerprinting Classification Performance". *2009 IEEE Int'l Conf on Communications (ICC09)*. Jun 2009.

59. Leest, A., and M. Bastiaans. "Gabor's Discrete Signal Expansion and the Discrete Gabor Transform on a Non-Separable Lattice". *2000 IEEE Int'l Conf on Acoustics, Speech, and Signal Processing (ICASSP00)*, 101–104. Jun 2000.

60. Li, Q. and W. Trappe. "Detecting Spoofing and Anomalous Traffic in Wireless Networks via Forge-Resistant Relationships". *IEEE Trans on Information Forensics and Security*, 2(4):793–808, Dec 2007.

61. Locke, G., and P. Gallagher. "NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 2.0". Special Publication 1108, National Institute of Standards, US Dept of Commerce, Feb 2012.

62. MacKay, D. *Information Theory, Inference, and Learning Algorithms*. Cambridge University Press, 2003.

63. Mann, S., and S. Haykin. "The Chirplet Transform: A Generalization of Gabor's Logon Transform". 205212. Proc. Vision Interface, Jun 1991.

64. Mendenhall, M., and E. Merenyi. "Relevance-Based Feature Extraction for Hyperspectral Images". *Neural Networks, IEEE Trans on*, 19(4):658–672, Apr 2008.

65. Neufeld J., C. Fifield, C. Doerr, A. Sheth, and D. Grunwald. "SoftMAC: Flexible Wireless Research Platform". 4th Workshop on Hot Topics in Networks, College Park, MD, Nov 2005.

66. Ozaktas, H., O. Arikan, M. Kutay, and B. Bonzagi. "Digital Computation of Fractional Fourier Transforms". *IEEE Trans on Signal Processing*, 44:2141–2150, 1996.

67. Pang, J., B. Greenstein, R. Gummadi, S. Seshan, and D. Wetherall. "802.11 User Fingerprinting". *13th Annual ACM Int'l Conf on Mobile Computing and Networking (MOBICOM07)*, 99–110. 2007.

68. Pei, S., and J. Ding. "Relations Between Gabor Transforms and Fractional Fourier Transforms and Their Applications for Signal Processing". *IEEE Trans on Signal Processing*, Vol. 55, No. 10, Oct 2007.

69. Pei, S., M. Yeh, and C. Tseng. "Discrete Fractional Fourier Transform Based on Orthogonal Projections". *IEEE Trans on Signal Processing*, 47:1335–1348, Oct 1999.

70. Proakis, J. *Digital Communications*. McGraw-Hill, New York, NY, 4th Edition, 2001. ISBN 0-07-232111-3.

71. Reising, D., and M. Temple. "WiMAX Mobile Subscriber Verification Using Gabor-Based RF-DNA Fingerprints". *2012 IEEE Int'l Communications Conf (ICC12)*. Jun 2012.

72. Reising, D., M. Temple, and J. Jackson. "Detecting Rogue Devices at Cloud Wireless Access Points Using RF Air Monitors". *Information Forensics and Security, IEEE Trans on*, 2012, UNDER REVIEW.

73. Reising, D., M. Temple, and J. Jackson. "Dimensionally Efficient ID Verification of OFDM-Based Devices Using GRLVQI Processing". *Journal on Selected Areas in Communications, IEEE*, 2012, UNDER REVIEW.

74. Reising, D., M. Temple, and M. Mendenhall. "Improved Wireless Security for GMSK-Based Devices Using RF Fingerprinting". *Int. J. Electronic Security and Digital Forensics*, Vol. 3, No. 1, pp. 41-59,2010.

75. Reising, D., M. Temple, and M. Mendenhall. "Improving Intra-Cellular Security Using Air Monitoring with RF Fingerprints". *2010 IEEE Wireless Communications & Networking Conf (WCNC10)*. Apr 2010.

76. Reising, D., M. Temple, and M. Oxley. "Gabor-Based RF-DNA Fingerprinting for Classifying 802.16e WiMAX Mobile Subscribers". 2012 IEEE Int'l Conf on Computing, Networking & Communications (ICNC12), Jan 2012.

77. Sato, A., and K. Yamada. "Generalized Relevance Learning Vector". *1995 Conf on Advances in Neural Information Processing Systems*, 423–429, 1996.

78. Sheng, Y., K. Tan, G. Chen, D. Kotz, and A. Campbell. "Detecting 802.11 MAC Layer Spoofing Using Received Signal Strength". 27th Conf on Computer Communications (INFOCOM08), Apr 2008.

79. Stockwell, R., L. Mansinha, and R. Lowe. "Localization of the Complex Spectrum: The $\mathbb{S}$ Transform". *IEEE Trans on Signal Processing*, 998–1001, Vol. 44, No. 4, Apr 1996.

80. Stouffer, K., J. Falco, and K. Scarfone. "Guide to Industrial Control Systems (ICS) Security". Special Publication 1108, National Institute of Standards, US Dept of Commerce, Jun 2011.

81. Suski, W. II, M. Temple, M. Mendenhall, and R. Mills. "RF Fingerprinting Commercial Communication Devices to Enhance Electronic Security". *Int. J. Electronic Security and Digital Forensics*, Vol. 1, No. 3, pp. 301-322, 2008.

82. Suski, W. II, M. Temple, M. Mendenhall, and R. Mills. "Using Spectral Fingerprints to Improve Wireless Network Security". 2008 IEEE Global Communications Conf (GLOBECOM08), Mar 2008.

83. Szmajda, M., K. Gorecki, and J. Mroczka. "Gabor Transform, SPWVD, Gabor-Wigner Transform and Wavelet Transform–Tools for Power Quality Monitoring". *Metrology and Measurement Systems*, Vol. 42, No. 3, Dec 2010.

84. Takahashi, D., Y. Xiao, Y. Zhang, P. Chatzimisios, and H. Chen. "IEEE 802.11 User Fingerprinting And Its Applications For Intrusion Detection". *Computers & Mathematics with Applications*, 60:307–318, 2010. Advances in Cryptography, Security and Applications for Future Computer Science.

85. Tarman, T., and E. Witzke. "Intrusion Detection Considerations for Switched Networks". *Enabling Technologies for Law Enforcement and Security*, 4232(1):85–92, 2001.

86. Tekbas, O., O. Ureten, and N. Serinken. "Improvement of Transmitter Identification System for Low SNR Transients". *IEE Electronics Letters*, Vol. 40, No. 3, pp. 182-183, Jul 2004.

87. Theodoridis, S., and K. Koutoumbas. *Pattern Recognition*. Academic Press, 4^{th} Edition, 2009.

88. Toonstra, J., and W. Kinsner. "A Radio Transmitter Fingerprinting System ODO-1". *Canadian Conf on Electrical and Computer Engineering*. Vol. 1, pp. 60-63, May 1996.

89. Toonstra, J., and W. Kinsnew. "Transient Analysis and Genetic Algorithms for Classification". *1995 IEEE Conf on Communications, Power and Computing (WESCANEX95)*. May 1995.

90. US Air Force Sensors Directorate (AFRL/RY),Wright-Patterson AFB, OH 45433. Mission Statement, www.wpafb.af.mil/afrl/ry/.

91. Von Dollen, D. "Report to NIST on the Smart Grid Interoperability Standards Roadmap". Jun 2009.

92. Wexler, J., and S. Raz. "Discrete Gabor Expansions". *Signal Processing*, Vol. 21, No. 3, pp. 207-220,1990.

93. Williams, M., M. Temple, and D. Reising. "Augmenting Bit-Level Network Security Using PHY Layer RF-DNA Fingerprinting". *2010 IEEE Global Communications Conf (GLOBECOM10)*. Dec 2010.

94. Williams, M., S. Munns, M. Temple, and M. Mendenhall. "RF-DNA Fingerprinting for Airport WiMax Communications Security". *4th Int'l Conf on Net and Sys Security (NSS10)*. Sep 2010.

95. Zanetti, D., B. Danev, and S. Capkun. "Physical-layer Identification of UHF RFID Tags". *16th Annual Int'l Conf on Mobile Computing and Networking (MOBICOM10)*, 353–364. 2010.

96. Zhenhai, D., X. Yuan, and J. Chandrashekar. "Controlling IP Spoofing Through Interdomain Packet Filters". *IEEE Trans on Dependable and Secure Computing*, 5(1):22–36, March 2008.

97. Zibulski, M., and Y. Zeevi. "Oversampling in the Gabor Scheme". *IEEE Trans. Signal Processing*, Vol. 41, No. 8, pp. 2679-2687,1993.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704–0188

The public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden to Department of Defense, Washington Headquarters Services, Directorate for Information Operations and Reports (0704–0188), 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202–4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number. **PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ADDRESS.**

1. REPORT DATE *(DD–MM–YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From — To)*
27–12–2012	Doctoral Dissertation	Oct 2009 — Dec 2012

4. TITLE AND SUBTITLE

Exploitation of RF-DNA for Device Classification and Verification Using GRLVQI Processing

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

Reising, Donald R., DR-II, AFRL/RY

5d. PROJECT NUMBER

JON# 11G186, 12G186, 13G266

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

Air Force Institute of Technology
Graduate School of Engineering and Management (AFIT/EN)
2950 Hobson Way
WPAFB OH 45433-7765

8. PERFORMING ORGANIZATION REPORT NUMBER

AFIT-ENG-DS-12-04

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)

Air Force Research Laboratory, AFMC
Attn: AFRL/RYWE (Dr. Vasu Chakravarthy)
2241 Avionics Circle, Bldg 620
WPAFB OH 45433-7734
(937)528-8269
Vasu.Chakravarthy@wpafb.af.mil

10. SPONSOR/MONITOR'S ACRONYM(S)

AFRL/RYWE

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION / AVAILABILITY STATEMENT

APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED

13. SUPPLEMENTARY NOTES

This material is declared a work of the U.S. Government and is not subject to copyright protection in the United States.

14. ABSTRACT

This dissertation introduces a GRLVQI classifier into an RF-DNA fingerprinting process and demonstrates applicability for device classification and ID verification. Unlike MDA/ML processing, GRLVQI provides a measure of feature relevance that enables Dimensional Reduction Analysis (DRA) to enhance the experimental-to-operational transition potential of RF-DNA fingerprinting. Using 2D Gabor Transform RF-DNA fingerprints extracted from experimentally collected OFDM-based 802.16 WiMAX and 802.11 WiFi device emissions, average GRLVQI classification accuracy of $\%C \geq 90\%$ is achieved using full and reduced dimensional feature sets at $SNR \geq 10.0$ dB and $SNR \geq 12.0$ dB, respectively. Performance with DRA$\approx$90% reduced feature sets included $\%C \geq 90\%$ for 1) WiMAX features at $SNR \geq 12.0$ dB and 2) WiFi features at $SNR \geq 13.0$ dB. For device ID verification with DRA$\approx$90% feature sets, GRLVQI enabled: 1) 100% ID verification of *authorized* WiMAX devices and 97% detection of spoofing attacks by *rogue* devices at $SNR = 18.0$ dB, and 2) 100% ID verification of *authorized* WiFi devices at $SNR = 15.0$ dB.

15. SUBJECT TERMS

RF-DNA, RF Fingerprinting, MDA/ML, GRLVQI, Verification, Classification, WiMAX, WiFi

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			Dr. Michael A. Temple
U	U	U	UU	146	19b. TELEPHONE NUMBER *(include area code)* (937) 255-3636,x4279, michael.temple@afit.edu